Deutscher Bundestag **Drucksache 16/8434**

16. Wahlperiode 28. 02. 2008

Unterrichtung

durch die Bundesregierung

Erfahrungsbericht über die praktische Umsetzung der §§ 100g, 100h der Strafprozessordnung

Der Deutsche Bundestag hat am 21. Oktober 2004 einen Entschließungsantrag auf Bundestagsdrucksache 15/3971 angenommen, mit dem die Bundesregierung aufgefordert wurde, dem Deutschen Bundestag bis zum 30. Juni 2007 einen Erfahrungsbericht über die praktische Umsetzung der §§ 100g, 100h der Strafprozessordnung (StPO) vorzulegen.

Um der Entschließung nachzukommen, hat das Bundesministerium der Justiz das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg (MPI) mit einer rechtstatsächlichen Untersuchung zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach den §§ 100g, 100h StPO“ beauftragt.

Mit Schreiben des Bundesministers der Justiz vom 27. Februar 2008 wurde dem Deutschen Bundestag der zu dieser Untersuchung erstellte Forschungsbericht des MPI zugeleitet. Bei der nachfolgend wiedergegebenen Fassung des Forschungsberichts handelt es sich um eine vom MPI am 12. März 2008 zur Verfügung gestellte, redaktionell überarbeitete Fassung, die auch in der vom MPI herausgegebenen Fachreihe „Kriminologische Forschungsberichte“ veröffentlich wird.

Zugeleitet mit Schreiben des Bundesministeriums der Justiz vom 27. Februar 2008 gemäß Beschluss vom 21. Oktober 2004 (Bundestagsdrucksache 15/3971).

Forschungsbericht des
Max-Planck-Instituts für ausländisches und internationales Strafrecht
– Forschungsgruppe Kriminologie –

Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h der Strafprozessordnung

Hans-Jörg Albrecht
Adina Grafe
Michael Kilchling

Freiburg i. Br., März 2008

Inhaltsverzeichnis

Seite

Seite

Seite

Seite

Seite

Seite

Seite

Hinweis zu gender mainstreaming

Zur leichteren Lesbarkeit der Texte wurde die männliche Form von personenbezogenen Hauptwörtern gewählt. Eine Benachteiligung des weiblichen Geschlechts ist damit nicht beabsichtigt.

1. Einleitung

A. Entwicklungen und Fragestellungen

Die vorliegende Untersuchung hat die Evaluation der Nutzung von Verkehrsdaten der Telekommunikation im Strafverfahren zum Gegenstand. Es geht um Fragen der Handhabung der §§ 100g, 100h StPO in der Praxis der Strafverfolgung und deren Auswirkungen im Strafverfahren. Bezug genommen wird dabei auf die normativen Grundlagen der Verkehrsdatenabfrage, ihre Entwicklung und Reform ebenso wie auf die sozialwissenschaftlichen Standards der Evaluationsforschung. Über die rechtstatsächlichen und evaluationsbezogenen Fragestellungen hinaus bietet die Verkehrdatenabfrage für die Kriminologie auch in theoretischer Hinsicht ein beträchtliches Potential. Hier geht es um die Analyse von Entwicklungen strafrechtlicher Sozialkontrolle, die ausgelöst werden durch Formen der organisierten und vernetzten Kriminalität. Da es sich bei dieser Kriminalität weitgehend um opferlose Kriminalität handelt, entfallen Anzeige und Zeugenaussagen als wesentliche Anknüpfungspunkte für Tatverdacht und die Einleitung strafrechtlicher Ermittlungen, Die strafrechtliche Sozialkontrolle formiert sich deshalb immer stärker um eine strategische und taktische Informationsgewinnung, die der Aufklärung von Phänomenen der opferlosen Transaktionskriminalität dient. Tansaktionskriminalität wie Drogen- und Menschenhandel, allerdings auch der (internationale) Terrorismus sind – anders als die klassische individuelle Kriminalität – auf kontinuierlichen Austausch von Informationen – im Kern Informationen zu Angebot und Nachfrage – angewiesen.[1] Transaktionskriminalität beruht auf Netzwerken von Akteuren sowie auf Mechanismen von Angebot und Nachfrage, der Rekrutierung, der Abstimmung, der Rechtfertigung, Propaganda und der Planung[2], die Ansätze für strategische Informationsgewinnung und Einzelfalluntersuchungen bieten.

Kriminalpolitik ist an der Evaluation von Gesetzgebung aus mehreren Gründen interessiert. Die rapide Veränderung der Kommunikation und ihrer technischen Grundlagen haben das Potential von Eingriffen in die Intimsphäre des Menschen drastisch erweitert, wie die Entscheidungen des Bundesverfassungsgerichts zur Wohnraum- und zur präventiven Telekommunikationsüberwachung ausgeführt haben.[3] Zwar werden die Verkehrsdaten der Telekommunikation, das heißt, interpretationsfähige Daten zu Ort, Zeit und Art der Kommunikation, zu den Kommunikationspartnern und Kommunikationsschwerpunkten im Allgemeinen als weniger sensibel als die Kommunikationsinhalte selbst eingeschätzt.[4] Doch ergibt sich aus der Gesamtheit der Verkehrsdaten ein Potential des Einsehens in das Private, das von persönlichen Beziehungen, Problemen und Präferenzen bis hin zu Bewegungsmustern reicht[5]. Vereinzelt wird deshalb auch bezweifelt, ob unter den Bedingungen digitaler Netzwerke der Kommunikation noch so trennscharf zwischen Inhalts- und Verkehrsdaten unterschieden werden kann, wie – international übereinstimmend und in der nicht anders durchführbaren Abstufung zu Inhaltsdaten der Telekommmmunikation nachvollziehbar und legitim – die Strafprozessgesetze voraussetzen.[6] Verkehrsdaten transportieren eben notwendigerweise und in unterschiedlichem Umfang auch Informationen zu den Inhalten der Beziehungen, der Kommunikation und aufgerufener Web Seiten.[7]

Die Untersuchung zu Telekommunikationsverkehrsdaten und ihrer Nutzung im Strafverfahren ist am Max-Planck-Institut für Ausländisches und Internationales Strafrecht eingebettet in eine Reihe von Studien zu dem Gebrauch neuer Ermittlungsmethoden und ihrem Stellenwert im modernen Strafprozess sowie in Systemen strafrechtlicher Sozialkontrolle. Untersuchungen zur Telekommunikationsüberwachung[8], zur Überwachung des Wohnraums[9] und zur Rasterfahndung[10] stehen neben Forschungen zu organisierter Kriminalität und ihrer Bewältigung durch Strafverfahren, in denen verdeckte Ermittlungsmethoden eine Schlüsselrolle spielen sollten[11]. Die Einführung von verdeckten (heimlichen) Ermittlungsmaßnahmen nicht nur in der Strafprozessordnung[12], sondern auch in den Polizeigesetzen der Länder verweist auf eine zunehmende Konvergenz zwischen Prävention und Repression ebenso wie auf die Konvergenz zwischen strategischer Informationsbeschaffung und einzelfallbezogenen Ermittlungen sowie diejenige zwischen innerer und äußerer Sicherheit[13]. Hieraus ergeben sich auch neue Arrangements des Datenaustauschs und der Datennutzung, die in den Beziehungen zwischen Geheimdiensten, Polizei und Strafverfolgungsbehörden Veränderungen hervorrufen[14]. Ausgelöst durch den dramatischen technologischen Fortschritt verändern sich Kommunikations- und Verhaltensmuster und damit Ausgangspunkte für Gefahrenabwehr und Strafverfolgung, die in den aus Informations- und Kommunikationstechnologien folgenden Datenströmen eine breite Ansatzfläche finden.[15] Verdeckte Ermittlungsmethoden tragen zu der deutlich erkennbaren Verschiebung der Gewichte von der Hauptverhandlung zum Ermittlungsver-

---

1 Vgl. den Forschungsstand in *Fijnaut/Paoli*, 2004.

2 Zu grundlegenden Konzepten vgl. *Arquilla/Ronfeldt*, 2001.

3 BVerfGE 109, S. 279 ff., zur akustischen Wohnraumüberwachung; Entscheidung des BVerfGs vom 27. Juli 2005, 1 BvR 668/04, NJW 2005, S. 2603ff. zum Schutz des Kernbereichs privater Lebensgestaltung für die Überwachung der Telekommunikation im präventiven Bereich, die auch für strafprozessuale Eingriffe Geltung hat.

4 *Caprioli/Saadoun/Cantero,* Rutgers Journal of Law & Urban Policy, 2006, S. 218; vgl. auch BVerfGE 107, S. 299ff sowie *Wolter,* SK StPO, 2006, § 100g Rn. 1: „kleine Telekommunikationsüberwachung“.

5 Vgl. hierzu die Ausführungen unter 2. D. IV. 3.

6 *Goemans/Dumortier*, 2003, S. 4.

7 Vgl. hierzu BVerfG, 1 BvR 330/96 vom 12.3.2003, Absatz-Nr. 71.

8 *Albrecht/Dorsch/Krüpe*, 2003.

9 *Meyer-Wieck*, 2005.

10 Pehl, 2007 (Zusammenfassung unter www.mpicc.de/ww/de/ext/forschung/forschungsarbeit/kriminologie/rasterfahndung.htm).

11 *Kinzig*, 2004; *Paoli/Fijnaut*, 2004; *Herz*, 2006.

12 Zur Entwicklung vgl. *Kinzig, J.*, 2004, S. 102ff.

13 *Kinzig, J.*, 2004, S. 128ff; zu den Entwicklungen in Ländern der Europäischen Union vgl. *Tak*, 2000, S. 1; Council of Europe, 2005, S. 39f.

14 *Albrecht*, *P.-A.*, 2000, S. 17f; vgl. ferner das Antiterrordateigesetz vom 22. Dezember 2006, BGBl. I S. 3409.

15 *Bignami*, Chicago Journal of International Law 2007, SSRN: http://ssrn.com/abstract=955261, S. 3.

fahren bei[16]. Die Verlagerung wird vor allem bei opferlosen Straftaten in einer proaktiven Orientierung der Polizei und der Strafverfolgungsbehörden sichtbar, zu der es keine Alternative gibt[17]. Sie kommt zum Ausdruck in dem Konzept von Initiativ- oder Strukturermittlungen und der Erforschung des Vorfelds der Kriminalität und sie ist Bestandteil einer Politik der Risikovorsorge, die vor allem der organisierten und transnationalen Kriminalität[18] und neuerdings dem internationalen Terrorismus gilt.[19]

Die Technik der Telekommunikationsüberwachung lässt dann beispielhaft die Eigenheiten verdeckter Ermittlungsmaßnahmen erkennen[20]:

– Verdeckte Ermittlungsmaßnahmen werden dem Tatverdächtigen nicht offenbart,

– erfassen teilweise eine Vielzahl von nicht verdächtigen Personen,

– sie generieren eine Vielzahl von Informationen, die nicht nur die Vergangenheit, sondern insbesondere die Zukunft oder das Vorfeld bzw. die Vorläufer von Straftaten betreffen,

– sie können Informationen unabhängig von Zeugnisverweigerungsrechten dritter Personen erfassen,

– sie erfassen Informationen unabhängig davon, wie intim und vertraulich die Kommunikation auch ist.

Mit der Umsetzung der Europäischen Richtlinie zur Speicherung von Telekommunikationsverkehrsdaten aus dem Jahre 2006[21] wird im Raum der Europäischen Union eine Steigerung insoweit sichtbar, als nunmehr im Wege der Vorratsspeicherung Verkehrsdaten der Telekommunikation (wie in Artikel 5 der Richtlinie 2006/24/EG festgelegt) für mindestens sechs Monate und höchstens zwei Jahre durch die Telekommunikationsanbieter gespeichert bleiben und für Zwecke der Strafverfolgung vorgehalten werden sollen. Die Datenerfassung betrifft Mobiltelefone ebenso wie Verbindungen, die über das Internet zustande kommen, und wird damit beständig und über die bereits heute zu Abrechnungszwecken erfassten Daten hinausgehend zu einer umfassenden Vorratsspeicherung von Verkehrsdaten in den Mitgliedsländern der Europäischen Union führen.

Die Verabschiedung der Europäischen Richtlinie zur Telekommunikationsverkehrsdatenspeicherung im Jahr 2006 hat eine länderübergreifende Auseinandersetzung zu einem vorläufigen Abschluss gebracht, in die neben Strafverfolgungsbehörden, Geheimdiensten, Kriminalpolitik auch Datenschutzbeauftragte, Nichtregierungsorganisationen mit menschenrechtlichem Schwerpunkt, Telekommunikationsunternehmen, Journalistenverbände und Strafrechtswissenschaftler sowie Kriminologen einbezogen sind.[22] Die europäischen rechtspolitischen Diskurse verweisen in den Schwerpunkten auf die unterschiedlichen Interessenlagen von Akteuren, auf das Speichern von Daten für Zwecke der Repression und Prävention, den Stellenwert des Persönlichkeitsrecht in einer umfassenden Sicherheitspolitik und ferner auf die Frage, wie weit private Sektoren in Unternehmungen der repressiven und präventiven Kontrolle der Kriminalität verpflichtet werden dürfen.[23]

Der Zugriff auf Telekommunikationsverkehrsdaten ist ein Ermittlungsinstrument, dem in neuerer Zeit neben der Überwachung der Kommunikationsinhalte eine zunehmende Bedeutung zugeordnet wird. Eine zentrale Rolle spielen Verkehrsdaten in der Bekämpfung der Datennetzkriminalität. Jedoch dürften Verkehrsdaten nunmehr angesichts der sich dramatisch verdichtenden digitalen Kommunikation für Ermittlungen in fast allen Bereichen der Kriminalität von Belang sein. Sie können zur Bestimmung des Aufenthaltsorts von Personen, zur Beweisermittlung oder zur Offenlegung von Täterstrukturen und Netzwerken der Transaktionskriminalität dienen. Verkehrsdaten werden von der Praxis weithin – wie nicht zuletzt die Richtlinie der Europäischen Union für die Vorratsspeicherung (2006/24/EG), der darauf bezogene Regierungsentwurf vom 27. Juni 2007 (Bundestagsdrucksache 16/5846) und das zum 1. Januar 2008 getretene Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (Bundesgesetzblatt 2007, I, Nr. 70, S. 3198) demonstrieren – als unverzichtbare Informationsquelle angesehen.

Nicht zuletzt nehmen die Bestandsdaten zur Telekommunikation, also die durch § 3 Nr. 3 TKG (2004) definierten Informationen zur Person von Telekommunikationsteilnehmern, im Zusammenhang mit automatisierter und manueller Auskunft nach §§ 112, 113 TKG (2004) eine bedeutsame Rolle ein. Nach der von der Bundesregierung im Verfassungsbeschwerdeverfahren 1 BvR 1299/05, in dem die Verfassungswidrigkeit der Speicherung und der Auskunft von Bestandsdaten geltend gemacht wird, vorgetragenen Auffassung haben die §§ 112, 113 TKG eine vergleichbare Funktion wie die entsprechenden Regelungen zum Kraftfahrzeug- und Melderegister sowie zur automatisierten Kontenabfrage nach § 24c KWG und fügen sich insoweit in vorhandene Strukturen der Erfassung, Aufbereitung und des Zugangs zu persönlichen Daten im nationalen Recht ein.[24] Die Einrichtung von Dateien mit Bestandsdaten der Telekommunikation lässt sich europaweit und international beobachten. So wird in den Niederlanden ein zentrales, beim Justizministerium angesiedeltes Informationssystem (Centraal Informatiepunt Opsporing

[16] So schon Wolter, J., 1991, S. 35f;

[17] Brenner, International Journal of Communications Law & Policy 2004, SSRN: http://ssrn.com/abstract=623283.

[18] *Albrecht*, Angewandte Sozialforschung 2002, S. 135f; *Kinzig*, 2004, S. 122ff.

[19] Zusammenfassend *Council of Europe*, 2005.

[20] Vgl. hierzu *auch Council of Europe*, 2005, S. 13–17.

[21] Richtlinie 2006/24/EG der Europäischen Union zur Speicherung und Nutzung von Telekommunikationsverkehrsdaten.

[22] *Büllingen/Gillet/Gries/Hillebrand/Stamm,* 2004*; KPMG Informatie Risk Management,* 2004*; Breyer* 2005*; Nuno Alvaro,* 2005; *Larnhof,* 2006.

[23] *Steinhardt*, Journal of Contingencies and Crisis Management 2003; *Peissl*, Journal of Contingencies and Crisis Management 2003; *Kinzig*, 2004.

[24] Stellungnahme vom 22. Januar 2007, S. 16 ff, www.daten-speicherung.de/data/TKG-StN.pdf.

Telecommunicatie (CIOT, Zentrale Informationsstelle für die Ermittlungen in Telekommunikationsangelegenheiten) aufgebaut, mit dem mittelfristig alle Telekommunikationsinformationen, einschließlich des Internets, zusammengefasst und der Polizei, den Geheimdiensten und der Justiz zugänglich werden sollen.[25] In Australien werden die entsprechenden Informationen in einer „Integrierten Öffentlichen Adressdatenbank" (Telecommunications Act 1997, Teil 4) zusammengeführt. Informationssysteme, die die Identifizierung und die Wohnortbestimmung von Personen über ihre Kommunikationsmittel ermöglichen, zeigen an, dass sich das Kommunikations- und Informationsverarbeitungsverhalten der Gesellschaft im letzten Jahrzehnt erheblich verändert hat. Die Entwicklungen verweisen auch darauf, dass die konventionellen Register der Meldebehörden und Kraftfahrzeugverwaltung zwar nicht ihre Bedeutung verlieren werden. In den Vordergrund dürften sich jedoch in der Zukunft zentrale Kommunikationsanschlussverzeichnisse schieben.[26] Dies liegt in dynamischen Nutzungsmöglichkeiten begründet, die den konventionellen Registern nicht eigen sind.

Das Telefonieren über das Internet (Voice over IP) ist nicht nur ein Beispiel für Fortschritte in der Kommunikationstechnologie, sondern auch für Konvergenz von Telekommunikationsmedien[27]. Das Internet hat die Möglichkeit eröffnet, Alltagsgeschäfte wie Einkauf und Banküberweisungen auf elektronischem Wege vorzunehmen. Die Zahl der Mobilfunkanschlüsse nahm zwischen Mitte der 1990er Jahre und 2006 stetig zu.[28] In den nächsten Jahren wird eine Sättigung der Gesellschaft mit mobiler Kommunikation eintreten. Zunehmend verfügen Personen über mehrere Rufnummern und über mehrere technische Möglichkeiten auch mobiler Telekommunikation. Der Trend geht im Übrigen als Konsequenz der Breitbandtechnologie zu einer erheblichen Beschleunigung und Erweiterung der Datenübertragung.

Insbesondere die Digitalisierung der Kommunikation hat aber dazu geführt, dass beim Austausch von Informationen speicherungsfähige und aussagekräftige Spuren hinterlassen werden. Denn zum Zwecke der Rechnungsstellung wird von den Telekommunikationsanbietern gespeichert, wann von welcher Rufnummer aus mit welchen anderen Rufnummern wie lange Verbindungen bestanden. Standort und Bewegungen werden teilweise festgehalten. Mittels der jedem Mobiltelefon zugehörigen elektronischen Gerätekennung (IMEI) lässt sich der Ort der Einwahl in eine Funkzelle lokalisieren. Ähnlich verhält es sich im Internet. Immer wenn eine Verbindung in das Internet erfolgt, wird eine IP-Adresse zugewiesen. Für betriebliche Zwecke gespeicherte Verkehrsdaten sind für Ermittlungszwecke und zur Beweisführung geeignet, sie können im Übrigen auch zur Verbesserung von Notrufsystemen und für weitere Zielsetzungen Verwendung finden.[29]

Mit den technischen Möglichkeiten verändern sich ferner Gelegenheitsstrukturen der Kriminalität. Internetstraftaten, wie beispielsweise das sog. Phishing, bei dem die Betroffenen von angeblichen Kreditinstituten per mail zur Eingabe der PIN-Nummer ihres Bankkontos aufgefordert werden, oder Betrug bei Internetversteigerungen beruhen auf den durch die moderne Kommunikationstechnologie geschaffenen Strukturen. Überall dort, wo Transaktionen den Kern der Straftaten bestimmen, verändert die Kommunikationstechnologie die Straftaten sowie das Gesamtbild der Kriminalität. Das Täterverhalten und die Tatphänomenologie spiegeln die Entwicklung der Kommunikationstechnologie selbstverständlich wider. Gerade im Bereich der Transaktionskriminalität, zu der die Kernbereiche der organisierten Kriminalität zu rechnen sind, erfolgen Anpassungen – theoretisch bestimmbar als rationale Entscheidungen (rational choice) –, die die Transaktionskosten, die im Wesentlichen aus dem Entdeckungsrisiko bestehen, verringern sollen. Die Anpassungen lassen sich deskriptiv erfassen; hierzu zählen neben dem Wechsel von Mobiltelefonen und deren Beschaffung durch „Strohmänner" der Tausch von SIM-Karten, der Einsatz von Prepaid-Karten oder die Verwendung ausländischer Geräte im Roamingverfahren. Spuren können schließlich durch Verschlüsselungstechniken verwischt werden.[30] Theoretisch handelt es sich insoweit um erwartbare Veränderungen, als diese recht einfach über rationale Kalküle vorhergesagt werden.

B. Veränderungen strafrechtlicher Sozialkontrolle

Die Entwicklungen der Kommunikationstechnologie und das veränderte Kommunikationsverhalten führen auch zu einer Erweiterung des Potentials für Überwachung, Gefahrenvorsorge und Strafverfolgung. Gerade die Verkehrsdatenabfrage und die Telekommunikationsüberwachung gewinnen nach Auffassung der Strafverfolgungsbehörden zunehmend an Bedeutung. Anhand von Verkehrsdaten kann zum Beispiel abgelesen werden, von welchen Mobilfunkanschlüssen in der Nähe eines Tatorts zur Tatzeit telefoniert worden ist oder mit welchem Anschluss das Opfer eines Tötungsdelikts vor der Tat Kontakt hatte. Bewegungsprofile und Verbindungsmuster erleichtern die Einsicht in Zusammenhänge zwischen Straftaten und Tätern, auch in Kontaktstrukturen, die unbeteiligte Dritte einschließen.[31]

Die Entwicklungen im Bereich der Telekommunikationsüberwachung und verdeckter Ermittlungen allgemein verweisen auf grundlegende Veränderungen in Systemen sozialer Kontrolle. Gary T. Marx, ein amerikanischer Kriminologe, hat sich in einer Arbeit aus den 1980er Jahren aus einer über die bis dahin vorherrschenden dogmatischen und rechtspolitischen Analysen hinausgehenden Perspektive mit proaktiven und verdeckten Ermittlungs-

---

[25] Opinion from the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] Legislative proposal (Bill) for implementation of the European Directive on Data Retention. Pertaining to the tender letter of 22 January 2007.

[26] Im Jahr 2006 belief sich die Zahl der Abfragen aus der zentralen Bestandsdatenbank der Telekommunikation durch Sicherheitsbehörden auf 3,6 Millionen; Bundesnetzagentur, Jahresbericht 2006, S. 103.

[27] Zusammenfassend *OECD,* 2007.

[28] *OECD,* 2007, S. 97–101.

[29] Vgl. die Übersichten in *Gow/Ihnat*, Surveillance & Society 2004

[30] Vgl. hierzu zusammenfassend *Nuno Alvaro*, 2005.

[31] *Danezis/Wittneben*, 2006.

methoden befasst. Er hat verdeckte Ermittlungsmethoden als wesentlichen Bestandteil einer „neuen Kontrolle“ bezeichnet[32] und damit Transformationsprozesse des Strafverfahrensrechts und der Strafverfolgungspraxis angesprochen, die seitdem noch deutlicher geworden sind. Noch in den 1970er Jahren wurde in Studien des Max-Planck-Instituts für die Ermittlungstätigkeit der Polizei eine ganz überwiegend reaktive Rolle nachgewiesen.[33] Dies hat sich über die letzten vierzig Jahre hinweg drastisch verändert. Die neue Kontrolle zielt auf bislang versteckt gebliebene Teile einer Realität (einvernehmlicher Transaktionen), die mit Hilfe neuer Informationstechnologie und proaktiver Strategien sichtbar gemacht werden. Ausgeleuchtet werden sollen Lebensbereiche, die dem reaktiven Ansatz der Strafverfolgung wegen des Fehlens von Anzeigeerstattern und aussagebereiter Zeugen verschlossen bleiben müssen. Ausgegriffen wird damit auch auf strategische Neuorientierungen der Strafverfolgung, in der sich Risikokontrolle und Prävention in den Vordergrund schieben.[34] Die grundsätzlichen Veränderungen werden ferner in einer Neubewertung von heimlichen und täuschenden Ermittlungspraktiken und umfassenden Informationssammlungen sichtbar. Historisch gesehen haben heimliche Informationserhebung und umfassende Informationssammlungene einstmals eine negative Bewertung deshalb erfahren, weil sie als regelmäßiger Bestandteil des Kontrollapparats repressiver und autoritärer Regime galten[35]. Die Neubewertung kommt in der international konsentierten Auffassung zum Ausdruck, dass heimliche Ermittlungsmaßnahmen für die Bekämpfung von schwerster Kriminalität und bei strenger Kontrolle ihrer Anwendung unerlässlich sind[36]. Jedoch bleibt ein Spannungsfeld, für das das Bundesverfassungsgericht immer wieder die Bedeutung der Gewissheit, nicht heimlich überwacht zu werden, als Garant für den aktiven Gebrauch der Menschenrechte durch die Bürger und als zentrales Element einer funktionierenden Demokratie betont. Nicht nur die Freiheit des Einzelnen, so das Bundesverfassungsgericht, kann durch eine stets präsente Gefahr heimlicher staatlicher Informationsbeschaffung wesentlich gehemmt werden. Heimliche staatliche Zugriffe beeinträchtigen auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist.[37]

Teil der von G. Marx beschriebenen neuen Kontrollpolitik ist darüber hinaus das rechtspolitische Insistieren auf Freiwilligkeit, Eigeninteresse und Zustimmung der Bürger zu einer präventiv und repressiv begründeten Ausweitung der Überwachung zu Zwecken der Gefahrenabwehr und der Strafverfolgung. Das Freiwilligkeitsverlangen beruft sich auf eine kommunitäre Ideologie und Mitwirkungsverpflichtungen der Bürger und der Zivilgesellschaft an der Herstellung von Sicherheit[38]. Gleichzeitig ist die Forderung freiwilliger Mitwirkung unterlegt mit Regeln, die eine Teilnahme an der Kontrolle erzwingen lassen. Dem liegt zugrunde, dass viele Bereiche der Zivilgesellschaft, insbesondere auch die Medien, Informationen erzeugen und über Wissen verfügen, die grundsätzlich für Strafverfolgungsbehörden, Polizei und Geheimdienste von erheblichem Interesse sind. Insoweit lässt sich eine Parallele herstellen zu der Geldwäschekontrolle, wo die Dritte Geldwäscherichtlinie der Europäischen Union heute nicht nur Banken und Finanzdienstleistern, sondern auch Rechtsanwälten und Notaren sowie einer Vielzahl anderer Geschäftsbereiche Kontroll- und Mitteilungspflichten dort auferlegt, wo sich der Verdacht der Geldwäsche oder der Terrorismusfinanzierung ergibt. Die Einbindung der Zivilgesellschaft in die Strafverfolgung und die Herstellung von Sicherheit wird tendenziell ausgeweitet. Dies zeigt sich auch in internationalen Entwicklungen. Im Jahr 2006 hat das australische Parlament ein Gesetz verabschiedet (Telecommunications Interception (Amendment) Act 2006), das die Überwachung von Telekommunikationsinhalts- und -Verkehrsdaten beträchtlich erweitert, und zwar prinzipiell auf unverdächtige Dritte, soweit die Sicherheitsbehörden davon ausgehen, dass auf diese Weise sicherheitsrelevante Informationen erlangt werden können. Ein besonderer Schutz der Presse oder anderer Berufsgeheimnisträger ist hierbei nicht vorgesehen. Während sich aus einer empirischen Perspektive die Veränderungen deutlich abzeichnen, ist die Frage, was die Veränderungen theoretisch und normativ bedeuten, einer kontroversen Diskussion ausgesetzt. Einerseits weisen Stimmen darauf hin, dass die Ausdehnung der verdeckten Ermittlungsmaßnahmen, insbesondere die Ausweitung der Überwachung der Telekommunikation, weder eine entsprechende Ausdehnung staatlicher Kontrolle über den Bürger[39] noch bedeutet, dass eine solche Kontrolle illegitim sei[40]. Ferner werden umfassende Informationen als Grundbedingung für eine funktionierende Strafverfolgung und vor allem für eine effektive Gefahrenabwehr hervorgehoben.[41] Andererseits werden der „gläserne“ Mensch, der autoritäre Sicherheitsstaat und eine unverhältnismäßige Beschränkung von Freiheitsrechten befürchtet.[42] Im Hintergrund steht jedoch ein Prozess der Ausweitung formeller und zunehmend technisch ausgerichteter Sozialkontrolle, der nicht zuletzt den auch im Begriff der Risikogesellschaft angesprochenen Verlust an informeller durch Familie, Nachbarschaft und die Einbindung in soziale Organisationen vermittelter Sozial- und Verhaltenskontrolle begleitet.

---

32 *Marx*, 1988, S. 206 ff.

33 *Steffen*, 1976; *Kürzinger*, 1978.

34 *Marx,* 1988, S. 217.

35 *Anechiarico/Jacobs,* 1996; *Ledergerber*, 2005; *Backes/Lindemann*, 2006.

36 Council of Europe, 2005, S. 13f.

37 BVerfGE 65, 1 ff; vgl. auch BVerfG, 2 BvR 1345/03 vom 22. August 2006 (zum IMSI Catcher); vergleichbar die Entscheidungsbegründung des United States District Court Eastern District of Michigan, Southern Division, Case No. 06-CV-10204, zum alle internationale Kommunikation in den USA erfassenden Überwachungsprogramm der Nationalen Sicherheitsbehörde (NSA), das sich auf Präsidentenerlasse stützte und kurz nach dem 11. September implementiert worden war.

38 Grundlegend *Etzioni*, 1995; *Ashworth*, 2002, S. 119 ff.

39 *Hess*, 2001, S. 333.

40 *Marx*, 1988, S. 233.

41 Vgl. beispw. *Volkmar*, Der Kriminalist 1997, S. 205, der die TelekommunikationsÜberwachung als eines der wirksamsten Instrumente kriminalistischen Handelns bezeichnet; freilich gibt es auch vorsichtigere Stimmen, wie Stellungnahmen in Ba-Wü LT Ds 11/4888 zu entnehmen ist.

42 *Covington/Burling*, 2003; *Farmer/Mann,* Technology Review 2004.

Die rechtspolitische Diskussion zur Verkehrsdatenerfassung, -speicherung und -nutzung ist durch Interessenkonflikte und -abwägungen gekennzeichnet. Auf der einen Seite stehen das aus dem Rechtsstaatsprinzip folgende Interesse an einer effektiven Strafverfolgung, der Schutz der Bürger vor Straftaten und damit die Gewährleistung von Sicherheit angesichts dynamischer Entwicklungen in den Phänomenen der Transaktionskriminalität und des Terrorismus. Auf der anderen Seite steht der Schutz der Grundrechte der Bürger, in die durch die Verkehrsdatenabfrage und andere verdeckte Ermittlungsmethoden eingegriffen wird.

Die rechtspolitischen Entwicklungen weisen zunächst ab Ende der 1980er Jahre angesichts der drastischen Erweiterungen der mit der Telekommunikation verbundenen personenbezogenen Daten auf eine erhebliche Sensibilisierung für den Schutz von Persönlichkeit und Privatsphäre hin. Dies lässt sich in den Dokumenten der Europäischen Union unschwer ablesen[43]. Freilich verändert sich die rechtspolitische Perspektive im Hinblick auf die Speicherung und den Zugriff auf Telekommunikationsdaten insbesondere nach dem 11. September 2001 schnell. Sicherheitsüberlegungen treten in den Vordergrund, dem Schutz der Privatsphäre – so eine plausible Diagnose – wird angesichts massiver Bedrohungsszenarien wird nunmehr geringeres Gewicht beigemessen.[44]

C. Grundrechte, Sicherheitspolitik und Evaluation

Im Mittelpunkt der verfassungsrechtlichen Diskussion stehen zunächst das Fernmeldegeheimnis (Artikel 10 GG), das Recht auf informationelle Selbstbestimmung und das allgemeine Persönlichkeitsrecht (Artikel 2 I i. V. m. Artikel 1 GG bzw. das Recht auf Privatheit, das über Artikel 8 EMRK den Bezugspunkt vor allem in europäischen Ländern ohne Verfassung bietet).[45] Der Schutz des Artikel 10 I GG umfasst neben dem Kommunikationsinhalt auch die Kommunikationsumstände, d. h. insbesondere, ob, wann und wie oft zwischen welchen Personen oder Anschlüssen Kommunikation stattgefunden hat oder versucht worden ist.[46] Gerade weil die Kommunikation sich immer mehr auf den Fernmeldeverkehr und elektronischen Schriftverkehr verlagert, lassen sich anhand der so entstehenden Verkehrsdaten aussagekräftige Informationen über Aufenthaltsorte, Kontaktmuster und Kommunikationsintensität des von einer Person genutzten Anschlusses gewinnen. Das Bundesverfassungsgericht hat immer wieder bekräftigt, dass die Nutzung des Kommunikationsmediums vertraulich möglich sein soll. Der effiziente Schutz des Fernmeldegeheimnisses verhindert, dass der Meinungs- und Informationsaustausch deshalb unterbleibt oder verändert verläuft, weil die Beteiligten damit rechnen müssen, dass sich staatliche Stellen in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen.[47] Die Vorratsdatenspeicherung erhöht nach Meinung von Datenschutzbeauftragten das Risiko unerwünschter Einflussnahme auf das Kommunikationsverhalten. Verwiesen wird aus der Perspektive des Datenschutzes auf die Gefahr der Entstehung eines Präventionsstaates, der seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr verlagert und dessen Informationsbedarf deshalb weit über die durch Tatverdacht oder konkrete Gefahren gezogenen Grenzen hinausreicht.[48] Das Bundesverfassungsgericht hat im Volkszählungsurteil[49] allerdings lediglich gegen eine Speicherung von Daten auf Vorrat zu nicht konkret definierten Zielen Stellung genommen. Mit diesen Vorgaben ist die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht vereinbar. Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind.[50] Demgegenüber ist die Vorratsdatenspeicherung mit dem allgemeinen Zweck der Strafverfolgung (Nutzbarkeit von personenbezogenen Daten für die Strafverfolgung in der Zukunft) begründet. Das Bundesverfassungsgericht hat auch auf die Besonderheiten hingewiesen, die sich aus der Verdecktheit bzw. Heimlichkeit der Ermittlungsmethoden ergeben. Wegen der Unbemerkbarkeit der Eingriffe in das Fernmeldegeheimnis und der Undurchsichtigkeit des anschließenden Datenverarbeitungsvorgangs für die Betroffenen gebietet Artikel 10 GG eine Kontrolle durch unabhängige staatliche Organe.[51] Gerade wegen der besonderen Schutzbedürftigkeit der Bürger, die aus dem Nichtwissen über einen Eingriff in ihre Grundrechte resultiert, bedarf es demnach einer effizienten Kontrolle der Überwachungsorgane und der Überwachungsmethoden.

Anlass zu rechtspolitischen Kontroversen bietet ferner die Inpflichtnahme Privater zu Strafverfolgungszwecken. Telekommunikationsanbieter werden bei der Telekommunikationsüberwachung und der Verkehrsdatenabfrage verpflichtet, Überwachungsmaßnahmen durchzuführen und Auskünfte zu erteilen. Strafverfolgung ist jedoch grundsätzlich originäre Aufgabe des Staates. Die Mitwirkung an der Strafverfolgung wird teilweise als Umsetzung einer staatsbürgerlichen Pflicht interpretiert, die staatliche Strafverfolgung nicht zu vereiteln (vgl. § 258 StGB). Eine Verantwortlichkeit wird aber auch für die Gewährleistung

---

[43] Vgl. hierzu Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Recommendation 3/97 on anonymity on the Internet (WP 6 – 5022/97); Working Party on the Protection of Individuals with regard to the Processing of Personal Data. Second Annual Report. Adopted by the Working Party on 30 November 1998, DG XVD/5047/98, final; zusammenfassend Warner, University of Ottawa Law & Technology Journal 2005.

[44] *Caprioli/Saadoun/Cantero,* Rutgers Journal of Law & Urban Policy 2006.

[45] *Ashworth*, 2002, S. 105 f.

[46] BVerfGE 65, S. 157, 172; BVerfGE 85, 386, 396; BVerfGE 100, S. 313, 358.

[47] BVerfGE 100, S. 313, 359.

[48] Entschließung der 72. Konferenz der DSB des Bundes und der Länder v. 26./27. Oktober 2006, Das Gewicht der Freiheit beim Kampf gegen den Terrorismus.

[49] BVerfGE 65, S. 1, 46.

[50] BVerfGE 65, S. 1, 46; BVerfGE 100, S. 313, 360.

[51] BVerfGE 30, S. 1, 23f., 30f.; BVerfGE 65, S. 1, 46; BVerfGE 67, S. 157, 185; BVerfGE 100, S. 313, 361.

der Strafverfolgung angenommen.[52] Andere bewerten dagegen zumindest die Tatsache, dass die Telekommunikationsanbieter teilweise auch zur Übernahme der Kosten für diese Strafverfolgungsmaßnahmen verpflichtet sind, als Eingriff in die Berufs- und Eigentumsfreiheit. Wenn der Staat sich Privater zur Umsetzung von Strafverfolgungsmaßnahmen bediene, dann müsse er auch die finanziellen Konsequenzen einer solchen Inpflichtnahme Privater tragen.[53]

Die Aufgabe der Kontrolle der Grundrechtseingriffe wird teilweise der Evaluation von Überwachungsmaßnahmen zugewiesen. Die Pflicht zur Evaluation gesetzlich begründeter Grundrechtseingriffe entsteht insbesondere im Bereich der Sicherheitsgesetzgebung dann, wenn bei der Einschätzung der Geeignetheit und Erforderlichkeit von zur Erreichung bestimmter Ziele gewählter Mittel auf Unsicherheiten in der Einschätzung komplexer (organisierter) Kriminalität und erwarteter Auswirkungen von Ermittlungsbefugnissen zurückgehende Beurteilungsspielräume genutzt wurden.[54] Denn ein Gesetz kann wegen Unsicherheiten des gegenwärtigen Erkenntnisstandes verfassungsmäßig sein, aber durch einen verbesserten oder durch neue Entwicklungen veränderten künftigen Erkenntnisstand eine veränderte Beurteilung in verfassungsrechtlicher Hinsicht erfahren.[55] Eine erfahrungsgestützte Evaluation dient demnach dazu, das zum Zeitpunkt des Gesetzesbeschlusses bestehende Informationsdefizit nachträglich auszugleichen und die ursprüngliche Prognose zu überprüfen.[56] Auch der Bundesdatenschutzbeauftragte Peter Schaar misst einer unabhängigen Evaluation sowohl der Rechtsvorschriften als auch der Maßnahmen mit besonderer Eingriffstiefe eine besondere Bedeutung zu.[57] Die mehrfache Befristung der Regelungen zur Verkehrsdatenabfrage – sowohl der Vorgängervorschrift des § 12 FAG (Finanzausgleichgesetz) als auch der jetzigen Vorschriften der §§ 100g, 100h StPO – zeigt, dass der Gesetzgeber gerade diese Maßnahme für noch nicht abschließend regelungsfähig hielt und sie erst einer eingehenden Überprüfung unterziehen wollte.

D. Ziele der Untersuchung

Ziel der vorliegenden Untersuchung ist die Evaluation der Verkehrsdatenabfrage im Rahmen der §§ 100g, 100h StPO. Im Zentrum stehen die Antrags- und Anordnungspraxis der Auskunftserteilung, die Nutzung der erteilten Auskünfte sowie die Effizienz des Ermittlungsinstruments, auch in Kombination mit anderen Ermittlungsmaßnahmen. Dabei geht es um die Ermittlung von Grunddaten zur Praxis der Anordnungen, der Anzahl der Betroffenen sowie um Anlass und Ergebnisse der Maßnahmen. Es soll erforscht werden, in welchem Umfang die Verkehrsdatenabfrage in der Praxis angewandt wird und in welchem Verhältnis sie zu anderen Ermittlungsmethoden steht. Fraglich ist, ob die Anordnungsvoraussetzungen hinreichend berücksichtigt werden und eine Begründung der Maßnahmen durch Polizei und Justiz erfolgt. Des Weiteren wird erhoben, welche Straftaten den Anordnungen zugrunde liegen. Von besonderem Interesse ist hier die Frage, ob Kinderpornographie, Organisierte Kriminalität und Rauschgiftdelikte die ausschlaggebenden Deliktsbereiche darstellen, wie in der Rechtspolitik hervorgehoben wird, oder ob die Schwerpunkte in anderen Kriminalitätsbereichen liegen. Von Bedeutung ist auch die Frage, ob der Eingriff durch die verdeckte Ermittlungsmaßnahme in einem angemessenen Verhältnis zum Eingriffszweck steht und ob sie – soweit die Zielwahlsuche (§ 100g II StPO) bzw. die Funkzellenabfrage (§ 100h II Satz 2 StPO) betroffen sind – tatsächlich nur subsidiär angewandt wird. Hieraus folgt die Frage, welche Erfolge mit der Ermittlungsmethode erzielt werden können und ob der Eingriff in die Grundrechte der Beteiligten unter Effektivitätsgesichtspunkten gerechtfertigt ist. Weiter wird die Einhaltung der Benachrichtigungs- und Vernichtungspflichten Gegenstand der Untersuchungen sein. Darüber hinaus sollen rechtliche und praktische Anwendungsprobleme erforscht sowie etwaige Schwächen und Unklarheiten der Normen der §§ 100g, 100h StPO aufgedeckt und Verbesserungsvorschläge präsentiert werden.

Schließlich wird die Untersuchung Fragen der Einbeziehung Privater in den Strafverfolgungsprozess, d. h. der Verpflichtung der Telekommunikationsanbieter zur Auskunftserteilung über Verkehrsdaten, aufgreifen. Dabei werden der Ablauf der Anforderung von Verkehrsdaten und die Interaktionen zwischen Strafverfolgungsbehörden und Telekommunikationsanbietern untersucht. Ferner geht es um die Auswirkungen der Maßnahmen für die Netzbetreiber wie beispielsweise die bei der Durchführung entstehenden Kosten, ohne dass es Aufgabe der vorliegenden Untersuchung sein kann, hierzu belastbare Aussagen zu treffen. Mit diesem Problemkreis hängen die – ebenfalls nicht in den Kernbereich dieser Untersuchung fallenden – Fragen zusammen, inwieweit die Indienstnahme Privater zu Strafverfolgungszwecken verfassungsrechtlich zulässig ist und ob und in welchem Umfang den Anbietern die für sie entstandenen Kosten ersetzt werden, schließlich die Frage, ob eine Kostentragungspflicht der Telekommunikationsanbieter mit dem Grundgesetz vereinbar ist.

Im Bericht werden auch Fragen der Vorratsdatenspeicherung und ihrer Regelungen im Regierungsentwurf (Bundestagsdrucksache 16/5846) sowie in dem zum 1. Januar 2008 in Kraft getretenen Gesetz (Bundesgesetzblatt 2007, I, Nr. 70, S. 3198) aufgegriffen.

Die Studie knüpft an die bereits abgeschlossenen Untersuchungen des Max-Planck-Instituts für ausländisches und internationales Strafrechts zur „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen“ (1999 bis 2004) sowie zur „Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung („großer Lauschangriff“) nach § 100c I Nr. 3 StPO“ (2002 bis 2004) an. Sie ist Teil einer Schwerpunktsforschung, die sich mit der Rolle neuer und proaktiver, präventiv ausgerichteter Ermittlungsmethoden für die Ausbildung strafrechtlicher Sozialkontrolle insbesondere in den Feldern der Transaktionskriminalität befasst.

---

[52] Vgl. *Waechter*, VerwA 1996, S. 90.
[53] *Schmidt-Preuß*, 2005, S. 3.
[54] *Weinzierl*, 2006, S. 5.
[55] BVerfGE 90, S. 145 ff; *Albers*, 2005, S. 26.
[56] *Bizer*, KrimJ 2003, S. 290; vgl. zusammenfassend *Blum*, 2004.
[57] *Schaar,* MMR 2001, S. 714.

2. Rechtspolitische Entwicklungen und Stand der Forschung

A. Das verfassungsrechtliche Spannungsverhältnis von Persönlichkeitsrecht und Sicherheit

Aus einer internationalen Perspektive erweist sich in den rechtspolitischen Debatten der Konflikt zwischen Privatsphäre (privacy) und den Zugriffsmöglichkeiten auf Verkehrsdaten der Telekommunikation als zentral. Der Konflikt wird zuerst sichtbar in der Beantwortung der die Möglichkeit des Zugriffs auf Verkehrsdaten entscheidenden Frage, ob anonyme Telekommunikation grundsätzlich zugelassen werden soll oder nicht. Denn eine effiziente Abfrage gespeicherter Verkehrsdaten ist prinzipiell nur denkbar, wenn ein anonymer Zugang zur Kommunikation über digitale Netze ausgeschlossen wird. Die Entscheidung der Europäischen Union, Verkehrsdaten der Nutzung digitaler Netze zwischen sechs Monaten und zwei Jahren zu speichern, setzt deshalb voraus, dass ein anonymer Zugang unzulässig ist und auch praktisch verhindert wird. Dabei geht es auch um die Zukunft des (anonymen) „Prepaid“ Zugangs zur Kommunikation, dessen Anteil am Kommunikationsaufkommen ausweislich des OECD Berichts 2007 zur Entwicklung des Telekommunikationsmarkts in den OECD Ländern bei 42 Prozent liegt[58]. Insbesondere nach dem 11. September 2001 werden international Bestrebungen sichtbar, den Zugang zur Telekommunikation von einer Identifizierung der Nutzer abhängig zu machen und Telekommunikationsunternehmen zu verpflichten, bei Kauf des Zugangs Nutzerdaten zu erheben und zu speichern. Die Einführung des „Know your Customer“ Prinzips in Telekommunikationsgesetzgebungen hat in unterschiedlicher Art und Weise zu Erörterungen zu den allgemeinen Beziehungen zwischen dem Schutz der Privatsphäre und dem Interesse an effektiver Strafverfolgung vor allem in Fällen organisierter Kriminalität und des Terrorismus nach sich gezogen[59]. Hieraus werden bislang unterschiedliche Konsequenzen gezogen. Bislang hat sich eine Mehrheit der OECD-Länder dafür entschieden, einen anonymen Zugang zur Telekommunikation beizubehalten und auf die Feststellung der Identität von Telekommunikationsnutzern zu verzichten[60]. In Kanada und in Neuseeland haben Anhörungen zu Vorschlägen, Bestandsdaten zu registrieren und für Zwecke der Strafverfolgung und Gefahrenabwehr vorrätig zu halten, zum Abbruch der entsprechenden rechtspolitischen Bestrebungen geführt.

Waren Konflikte zwischen dem Schutz der Privatsphäre und der Erfassung von Bestandsdaten in den Ländern der Europäischen Union in der Vergangenheit wenig ausgeprägt[61], so hat der Normgebungsprozess der Europäischen Union zur Vorratsspeicherung von Verkehrsdaten eine noch andauernde Debatte über die Zukunft des Privaten in einem durch Sicherheitsbelange geprägten politischen Umfeld weiter angefacht[62].

[58] *OECD,* 2007, S. 99.
[59] *Centre for Policy Research on Science and Technology,* 2006, S. 20 ff.
[60] *Centre for Policy Research on Science and Technology,* 2006, S. 1f.
[61] Vgl. das Verfassungsbeschwerdeverfahren BvR 1299/05.
[62] *Sofsky*, 2007.

Bezogen auf Deutschland werden die Bedingungen für die Lösung der Konflikte – und damit der Spielraum für die Ausgestaltung der Überwachung und ihre Grenzen – maßgeblich durch die einschlägigen grundgesetzlichen Normen determiniert. Maßgeblich sind dabei, wie bereits angedeutet, Grundrechtspositionen sowohl der unmittelbar und mittelbar betroffenen Kommunikationsteilnehmer wie auch der – zwangsweise – in die Durchführung einbezogenen Telekommunikationsunternehmen.

I. Grundrechte der Telekommunikationsteilnehmer

Durch eine Vorratshaltung von Verkehrsdaten für Zwecke der Strafverfolgung sowie durch die Mitteilung von Daten auf der Grundlage von § 100g I Satz 1 StPO ist zunächst das Fernmeldegeheimnis aus Artikel 10 GG betroffen. Artikel 10 GG geht als spezielles Grundrecht dem Recht auf informationelle Selbstbestimmung der Telekommunikationsteilnehmer vor[63]. Bestandsdaten der Telekommunikation unterfallen dagegen ebenso wie bei nicht genutztem Mobilfunkbetrieb anfallende ortsbestimmende Daten[64] dem Schutzbereich des aus Artikel 2 in Verbindung mit Artikel 1 GG abgeleiteten Grundrecht auf informationelle Selbstbestimmung.

1. Das Fernmeldegeheimnis

Das Fernmeldegeheimnis schützt zwar in erster Linie den Kommunikationsinhalt, umfasst aber gleichfalls die Kommunikationsumstände. Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Anschlüssen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist.[65] Demnach sind auch die Verkehrsdaten als Umstände der Telekommunikation vom Schutz des Fernmeldegeheimnisses erfasst. Die Auskunft über Verkehrsdaten auf der Grundlage des § 100g StPO greift in den Schutzbereich des Artikel 10 GG ein.

Auch nicht verdächtige Telekommunikationsteilnehmer sind durch die Ermittlungsmaßnahme im Recht aus Artikel 10 GG tangiert. So werden bei der Zielwahlsuche gemäß § 100g II StPO, die auf die Ermittlung unbekannter Anschlussnummern, von denen Telekommunikationsverbindungen zu einem Anschluss des Beschuldigten oder des Nachrichtenmittlers nach § 100g I Satz 2 StPO hergestellt worden sind (= eingehender Telekommunikationsverkehr)[66], zielt, unbeteiligte Dritte erfasst. Zwangsläufig wird nicht nur der Anschluss des Beschuldigten oder des Nachrichtenmittlers überprüft, sondern es werden auch Daten von Nichtverdächtigen in die Maßnahme einbezogen. Denn alle Anschlüsse werden daraufhin untersucht, ob Verbindungen zu einem bestimmten Anschluss hergestellt worden sind. Insoweit handelt es sich um ein der

[63] *Leibholz/Rinck*, 2007, Artikel 10, Rn. 3.
[64] BGH (Ermittlungsrichter) Beschl. v. 21. Februar 2001 – 2 BGs 42/2001, StV 2001, S. 214; zusammenfassend *Demko*, NStZ 2004, S. 59 f.
[65] BVerfGE 67, S. 157, 172; BVerfGE 85, S. 386, 396; BVerfGE 100, S. 313, 358; BVerfG 1 BvR 330/96, Urteil vom 12.3.2003, S. 47; *Schäfer,* in: Löwe-Rosenberg, 2004, § 100g Rn. 3; *Leibholz/Rinck,* 2007, Artikel 10, Rn. 31.
[66] *Meyer-Goßner*, 2006, § 100g Rn. 11.

Rasterfahndung vergleichbares Verfahren, das letztlich durch ein Ausschlussverfahren zu einem umfassenden Kommunikationsprofil verdächtiger Personen führt.[67] Das Bundesverfassungsgericht hat den Eingriffscharakter bei den durch die Zielwahlsuche erfolgenden Zugriffen auf Telekommunikationsverkehrsdaten nicht verdächtiger Personen im Ergebnis allerdings als nicht grundrechtsrelevant eingestuft, da in der Praxis eine längerfristige Speicherung der Daten nur bei Treffern erfolgt.[68]

Nicht verdächtige Telekommunikationsteilnehmer sind auch bei der so genannten Funkzellenabfrage i. S. d. § 100h I Satz 2 StPO in ihren Grundrechten betroffen. Bei einer Funkzellenabfrage werden sämtliche Daten der Mobilfunkkommunikation aus einem bestimmten Raum (Funkzelle, in die sich ein Mobiltelefon eingeloggt hat) erhoben. Dabei werden die Verbindungs- und Bestandsdaten auch unverdächtiger oder nicht als Zeugen in Betracht kommender Personen erfasst.[69] Hinsichtlich der Größenordnung der Erfassung von Daten Unbeteiligter kommt es darauf an, auf welchen Raum sich die Funkzellenabfrage bezieht. Wenn beispielsweise eine Abfrage für den Berliner Hauptbahnhof tagsüber erfolgt, werden mehr Menschen von der Funkzellenabfrage erfasst als bei der Abfrage in einer ländlichen Region. Aufschluss über Größenordnungen geben beispielsweise anlässlich einer Sitzung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtags erörterte Fälle von Funkzellenabfragen in Ermittlungsverfahren wegen Brandstiftungs- und Tötungsdelikten.[70] Danach waren in einem Brandstiftungsverfahren etwa 700 Personen, die Mobiltelefone in einer relevanten Funkzelle zu einer bestimmten Zeit benutzt hatten, in die Ermittlungen einbezogen worden; in einem Verfahren wegen eines Tötungsdelikts waren mindestens 120 Mobilfunknutzer betroffen. Die Betroffenen, so wird in der parlamentarischen Debatte hervorgehoben, befanden sich erwartungsgemäß zunächst in einer Lage, in der durch zusätzliche Ermittlungen untersucht wurde, ob sie als Tatverdächtige, Zeugen oder eben Nichtverdächtige in Betracht kommen.

2. Das Recht auf informationelle Selbstbestimmung

Da Artikel 10 GG als spezielles Grundrecht vorgeht, kommt für die Verkehrsdatenabfrage das Recht auf informationelle Selbstbestimmung (Artikel 2 I i. V. m. 1 I GG) nicht unmittelbar in Betracht.[71] Jedoch lassen sich die Grundsätze, die sich aus dem das Recht auf informationelle Selbstbestimmung ausführenden Urteil des Bundesverfassungsgerichts zum Volkszählungsurteil ergeben, auf den Umgang mit Verkehrsdaten anwenden.[72] Danach hat der Bürger das Recht, darüber zu entscheiden, welche personenbezogenen Daten erhoben, verarbeitet oder Dritten mitgeteilt werden.[73] Bei der Auskunftserteilung nach §§ 100g, 100h StPO wird in dieses Recht durch die Weitergabe der Daten der dazu verpflichteten Telekommunikationsunternehmen an die Behörden eingegriffen. Die Telekommunikationsteilnehmer können in einem solchen Fall gerade nicht darüber entscheiden, ob die Daten weitergegeben werden oder nicht. Sie werden an diesem Entscheidungsvorgang nicht beteiligt. Mit der Umsetzung der Europäischen Richtlinie 2006/24/EG wird dieser Eingriff erweitert werden. Denn auf dieser Grundlage sollen neben den Bestandsdaten auch alle wesentlichen Verkehrsdaten der Telekommunikation für bestimmte Zeiträume erhoben und gespeichert werden.

3. Verfassungsrechtliche Legitimation

Eingriffe in das Fernmeldegeheimnis und in das Recht auf informationelle Selbstbestimmung verlangen zunächst ein förmliches Gesetz[74], das für den Fall der Verkehrsdatenabfrage in Gestalt der §§ 100g, 100h StPO vorliegt. Wie bei jedem staatlichen Eingriff muss jedoch auch bei der Verkehrsdatenabfrage die Verhältnismäßigkeit gewahrt sein. Gerade wegen der hohen Anzahl an unbeteiligten Betroffenen wurde im Gesetz die Verhältnismäßigkeit durch das Erfordernis der Subsidiarität für die Funkzellenabfrage und die Zielwahlsuche konkretisiert. Gerade bei einer verdeckten Ermittlungsmethode, die eine Vielzahl von Personen betrifft, spielt die Verhältnismäßigkeitsprüfung eine ausschlaggebende Rolle. Sie sichert die Schaffung eines Gleichgewichts zwischen der durch die Ermittlungsmaßnahme geförderten Sicherheit der Bürger und der dadurch gleichzeitig bewirkten Einschränkung der Grundfreiheiten. Die Verhältnismäßigkeit setzt zum einen die Eignung der Maßnahme zur Verfolgung eines legitimen Zwecks voraus. Legitimer Zweck der Ermittlungsmaßnahme ist die Strafverfolgung (unterlegt selbstverständlich mit dem Ziel, Rechtsgüterschutz zu leisten bzw. Sicherheit zu schaffen). Näher differenziert wird die Legitimität des Schutzzwecks durch die Bestimmung der Einzelziele, die mit der konkreten Maßnahme verfolgt werden. Geeignet ist die Maßnahme dann, wenn das vom Staat gewählte Mittel zur Erreichung des konkreten Zwecks tauglich ist.[75] Die Eignung lässt sich überprüfen, in dem die Erfolgsquote der Ermittlungsmethode bestimmt, also nachgewiesen wird, dass die Abfrage von Verkehrsdaten die Ermittlungstätigkeit fördert. Des Weiteren setzt die Verhältnismäßigkeit voraus, dass kein milderes und gleichermaßen geeignetes Mittel zur Zielerreichung vorhanden ist, die Maßnahme also erforderlich ist. Für dieses Element lassen sich Indikatoren bilden, die aus der Überprüfung der Effizienz der Maßnahme und der relativen Bedeutung der Verkehrsdatenab-

[67] *Weßlau*, ZStW 113 (2001), S. 693; kritisch unter Hinweis auf eine wegen bloßer Willkürkontrolle durch Revisionsgerichte nur unzureichenden Wirkung der Subsidiaritätsklausel des § 100 g II StPO *Wolter*, in: SK StPO, 2006, § 100g, Rn. 8.

[68] BVerfG NJW 2003, S. 1787, 1793 unter Verweis auf BVerfGE 100, S. 313, 366.

[69] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 28.

[70] Schleswig-Holsteinischer Landtag Stenographischer Dienst und Ausschussdienst, Niederschrift, Innen- und Rechtsausschuss, 16. WP – 5. Sitzung, 7. September 2005, S. 4ff.

[71] *Nack*, in: Karlsruher Kommentar, 2003, § 100g Rn. 1.

[72] BVerGE 65, S. 44 ff; *Leibholz/Rinck*, 2007, Artikel 10, Rz. 41.

[73] BVerfGE 65, S. 42; *Holznagel/Enaux/Nienhaus*, 2006, S. 254.

[74] *Dreier,* in: Dreier, 2004, Artikel 2 I Rn. 86.

[75] *Dreier*, in: Dreier, 2004, Vorb. Rn. 147.

frage im Verhältnis zu anderen Ermittlungsmaßnahmen folgen. Freilich können solche Indikatoren, die aus Strafverfahrensakten, Befragung und Interview gezogen werden können, nicht gleichgesetzt werden mit einer direkten Beobachtung der allein auf eine einzelne Ermittlungsmaßnahme zurückführbaren Wirkungen. Eine direkte Beobachtung und damit eine unmittelbare Entscheidung darüber, welche Annahme zur Erforderlichkeit zutrifft, könnte nur über ein kontrolliertes Experiment erfolgen[76], in dem die Rahmenbedingungen gleich gehalten und lediglich die Interventionen variiert werden.[77] Ein kontrolliertes Experiment ist freilich nicht durchführbar. Entsprechendes gilt für (weniger „harte“) Verfahren der Nutzung „natürlicher“ Experimente. Die Bildung von Kontrollgruppen, die in anderen Bereichen strafrechtlicher Interventionen (insbesondere strafrechtlicher Sanktionen) einen, wenn auch nicht gleichwertigen, Ersatz für kontrollierte Experimente schaffen soll, ist im Feld der empirischen Strafverfahrensforschung jedenfalls dann nicht möglich, wenn es um verdeckte Ermittlungsmethoden geht.[78] Es bleibt allein die Identifizierung geeigneter Indikatoren des Nutzens, die sich aus Dokumentenanalyse und Interview ziehen lassen.

Schließlich muss die Maßnahme verhältnismäßig im engeren Sinne sein. Die Antwort auf die Frage der Verhältnismäßigkeit im Engeren setzt Abwägungen zwischen den betroffenen Interessen voraus und damit eine Evaluation der Eingriffsfläche und Eingriffstiefe des Instrumentes sowie seiner relativen Beiträge zur Förderung der strafrechtlichen Ermittlungen. Jedoch ist diese Messung durch die prinzipiell eröffneten empirischen Zugänge zu den Ermittlungsmaßnahmen begrenzt. Eine begleitende Beobachtung, die um die empirischen Produkte der Ermittlungen ergänzt wäre (und damit tatsächlich für verschiedene Ermittlungsmaßnahmen repräsentativ Nutzen und Eingriffstiefe erfassen könnte), kann im Feld der verdeckten und technischen Ermittlungsmaßnahmen jedoch nicht umgesetzt werden. *Albers* und *Bize*[79] haben sich in diesem Punkt zur Untersuchung der Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung kritisch geäußert.[80] Freilich ist über die in diesem Feld einsetzbaren Methoden der Sozialforschung, nämlich Dokumentenanalyse und Interview, nicht vollständig überprüfungsfähig, wie die Streubreite der Maßnahme und die Eingriffstiefe in dem von den Autoren beschriebenen Sinne ausgestaltet sind. *Albers* ist beispielsweise der Ansicht, dass festgestellt werden müsse, wie viele unbeteiligte Dritte wie häufig vom Einsatz einer Methode betroffen sind[81]. Im Übrigen wäre natürlich für die Eingriffstiefe auch entscheidend, welche Art der Kommunikation bzw. der Kontakte und welche Inhalte erfasst werden. Dies lässt sich jedoch beispielsweise bei einer Funkzellenabfrage im Bereich eines Bahnhofes über einen längeren Zeitraum schwer und vor allem nicht zuverlässig feststellen. Ebenso wenig ist die Erhebung dieser Information bei einer Telekommunikationsüberwachung beispielsweise über mehrere Monate möglich. Zuverlässig feststellen lässt sich nur, wer unmittelbar von der Maßnahme betroffen war, d. h. der Beschuldigte, etwaige andere Anschlussinhaber und -nutzer sowie Nachrichtenmittler. Die Argumentation von *Albers und Bizer* verkennt außerdem, welche Veränderungen die stetig wachsende Zahl an Festnetz- und Mobilfunkanschlüssen mit sich bringt. In Zeiten der modernen Kommunikation verfügen die meisten Personen über mehrere Telefone bzw. Rufnummern (z. B. bei einem ISDN-Anschluss). Im Rahmen von Telekommunikationsüberwachungen und vor allem von Verkehrsdatenabfragen ist die Identität der in irgendeiner Form betroffenen Personen häufig nicht bekannt und es lässt sich kaum feststellen, wie viele Nummern einer Person zugeordnet werden können. Insofern wäre eine Bestimmung der Anzahl mittelbar Betroffener nicht präzise durchführbar. Der zweite Gesichtspunkt, der für die Angemessenheit relevant ist, bezieht sich selbstverständlich auf den Erfolg der Maßnahme. Der Erfolg kann auf verschiedenen Ebenen abgelegt sein. Auch hier stellen sich Probleme der Erfassbarkeit. Denn die Frage, ob mit dem Mittel der Verkehrsdatenabfrage Mehrwert in Form von mehr Sicherheit erzeugt wird, dürfte lediglich über subjektive Einschätzungen beantwortet werden können. Auf einer anderen Ebene liegt wiederum ein Erfolg, der sich als (kausaler) Beitrag zur Überführung eines Tatverdächtigen (oder zur Entlastung Beschuldigter) abbilden lässt. Schließlich kann auch an einen Erfolg gedacht werden, der sich in der simplen Machbarkeit von Überwachungsmaßnahmen äußert.[82]

Bei der Evaluierung der Verhältnismäßigkeit sollten auch – wie *Bizer* ausführt[83] – nachträgliche Vorkehrungen Berücksichtigung finden, die den Grundrechtseingriff möglichst effektiv begrenzen sowie sichtbar und damit überprüfungsfähig machen. Dies geschieht bei der Verkehrsdatenabfrage in Form der Benachrichtigungs- und Vernichtungspflicht. Zu berücksichtigen ist, dass die Zuordnung der Rufnummern zu einer bestimmten Person, die für eine Benachrichtigung notwendig wäre und meistens gar nicht vorgenommen wird, einen noch größeren Grundrechtseingriff darstellen würde. Der Sinn der Benachrichtigungspflicht besteht aber – auch – in einer Begrenzung des Grundrechtseingriffs und nicht in deren Verstärkung. Zusammenfassend lässt sich also sagen, dass die Evaluierung der Verhältnismäßigkeit von den Grenzen sozialwissenschaftlicher Datenerhebungsmethoden, den Grenzen eines Versuchsaufbaus sowie den Besonderheiten verdeckter Ermittlungsmethoden abhängig ist. Nicht zuletzt wird dies sichtbar in der Entwicklung empirischer Forschung zu Überwachungstechniken, die ganz wesentlich bestimmt ist durch qualitative Methoden.[84]

---

[76] Zusammenfassend *Ortmann,* 2002.
[77] Vgl. hierzu zusammenfassend *Bremer Institut für Kriminalpolitik,* 2000.
[78] Vgl. hierzu insbesondere *Dorsch,* 2005, S. 271ff.
[79] *Albers,* 2006, S. 32; *Bizer*, KrimJ 2003, S. 292.
[80] *Albrecht/Dorsch/Krüpe*, 2003..
[81] *Albers*, 2006, S. 32.
[82] Hierzu beispw. die vom *Bundesinnenministerium*, 2005, vorgelegte Evaluation der Terrorismusbekämpfungsgesetze.
[83] *Bizer*, KrimJ 2003, S. 291.
[84] Vgl. die in *Marx*, Law & Social Inquiry 2006, zusammengefasste Forschung.

II. Grundrechte der Telekommunikationsanbieter

Von den Anordnungen zur Verkehrsdatenabfrage sind auch Rechte der Telekommunikationsanbieter betroffen. Gemäß § 100g I Satz 1 StPO haben diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, aufgrund einer nach §§ 100g, 100h StPO ergangenen Anordnung unverzüglich Auskunft über die in § 100g III StPO bezeichneten Telekommunikationsverbindungsdaten zu erteilen, soweit die Auskunft für die Untersuchung erforderlich ist. Sie müssen Auskunft erteilen und haben im Falle der Weigerung sogar mit Sanktionen zu rechnen. Gemäß § 100h I Satz 3 i. V. m. §§ 95 II, 70 StPO können gegen den Mitwirkungsverpflichteten Ordnungs- und Zwangsmittel festgesetzt werden, wenn der Mitwirkungspflicht nicht nachgekommen wird. Insbesondere wegen der Verpflichtung zur unverzüglichen Auskunftserteilung kommt gar eine Strafbarkeit wegen Strafvereitelung in Betracht.[85] In Betracht kommen schließlich Eingriffe in Artikel 12 GG und Artikel 14 GG. Gemäß Artikel 19 III GG sind die Artikel 14 I GG und 12 I GG auch auf juristische Personen anwendbar.

1. Die Berufsfreiheit

Die gesetzliche Pflicht der Telekommunikationsanbieter, Auskunft über lediglich zu Rechnungszwecken gespeicherte Daten zu erteilen, berührt die in Artikel 12 GG verbürgte Freiheit, die Art und Weise der Berufsausübung selbst zu bestimmen. In der Rechtsprechung des Bundesverfassungsgerichts wird unterstrichen, dass sich die Indienstnahme Privater für öffentliche Aufgaben auch am Maßstab des Artikel 12 I GG messen lassen muss.[86]

2. Das Eigentumsrecht

Artikel 14 I GG schützt nicht nur die unmittelbare Herrschaft über den Eigentumsgegenstand, sondern auch Verfügungsfreiheit und Privatnützigkeit.[87] Zur Umsetzung der Pflicht der Übermittlung von Verkehrsdaten an Strafverfolgungsbehörden müssen aber Telekommunikationsanbieter in Hardware und Software investieren. Dabei handelt es sich um die Herstellung einer Infrastruktur zur Überwachung sowie deren dauerhafte Unterhaltung und Anpassung an technologische Entwicklungen. Sind die entsprechenden, zur Überwachung geeigneten Einrichtungen vorhanden, so müssen diese nach Maßgabe der gesetzlichen Vorschriften genutzt werden.[88] Insoweit betrifft die Pflicht zur Anpassung des Betriebs an Erfordernisse der Überwachung und die Pflicht zur Übermittlung von Verkehrsdaten die im Schutzbereich des Eigentums liegende Eigentumsnutzungsfreiheit. Ob dies einen unzulässigen Eingriff in Artikel 14 I GG mit sich bringt, ist umstritten.[89] Für die Beurteilung von Eingriffen in Artikel 14 GG geht es jedoch – wie bei Eingriffen in die Berufsfreiheit – prinzipiell um die Verhältnismäßigkeit.[90]

3. Verfassungsrechtliche Legitimation

Grundsätzlich ist die Heranziehung Privater zur Erfüllung originär staatlicher Aufgaben nach einhelliger Auffassung zulässig[91], wenn vernünftige Erwägungen des Gemeinwohls die Heranziehung begründen. Herausragende Gemeinwohlbelange werden mit dem Ziel einer effektiven Strafverfolgung selbstverständlich angestrebt.[92] Eine besondere und die Verpflichtung zu Leistungen begründende Stellung der Telekommunikationsunternehmen folgt aus ihrer ausschließlichen Verfügungsmacht über Netze und Speichermedien. Im Übrigen wird auch das Interesse an einem wirksamen Geheimnisschutz genannt[93]. Die ausschließliche Verfügungsmacht sowie der Schutz der Daten der Kunden rechtfertigen daher die Indienstnahme der Telekommunikationsunternehmen als private Rechtssubjekte.[94] Die Grenze des verfassungsrechtlich Zulässigen ergibt sich aus dem Grundsatz der Verhältnismäßigkeit.[95] Umstritten ist allerdings die Frage, ob die Auferlegung der Kosten für die Vorhaltung der Infrastruktur der Überwachung sowie für die beständige Anpassung der Überwachungsinfrastruktur an den Stand der Technik entschädigungslos erfolgen darf.

B. Die gesetzliche Regelung der Verkehrsdatenabfrage

I. Entstehungsgeschichte

Seit 1. Januar 2002 ist die Verkehrsdatenabfrage in den §§ 100g, 100h StPO gesetzlich geregelt. Bis dahin befanden sich die gesetzlichen Grundlagen außerhalb der StPO, nämlich in § 12 FAG. Diese Vorschrift wurde, wie das gesamte Fernmeldeanlagengesetz, im Jahre 1928 geschaffen.[96] Geändert wurde das Gesetz unter anderem im Jahr 1989.[97] Die Verkehrsdatenabfrage nahm zu dieser Zeit verständlicherweise keine Bedeutung ein. Die fehlende praktische Relevanz beruhte darauf, dass im analogen Telefonsystem nach Beendigung des Kommunikationsvorgangs keine Informationen mehr über den Vorgang vorhanden waren. Dies führte zur weitgehenden Funktionslosigkeit des § 12 FAG.[98] Mit dem Prozess der Digitalisierung wuchs jedoch die Bedeutung der Verkehrsdatenabfrage, insbesondere auch deshalb, weil die Eingriffsermächtigung keine Begrenzung auf bestimmte Straftaten enthielt.[99] Gemäß § 12 FAG i. d. F. von 1989 konnten der

---

[85] *Nack,* in: Karlsruher Kommentar, § 100g Rn. 3.
[86] BVerfGE 30, S. 292, 311; BVerfGE 85, S. 329, 334.
[87] *Schmidt-Preuß*, 2005, S. 8.
[88] *Schmidt-Preuß*, 2005, S. 8.
[89] *Hammerstein*, MMR 2004, S. 223; *Kube/Schütze*, CR 2003, S. 667.
[90] *Hammerstein*, MMR 2004, S. 223.
[91] BVerfGE 30, S. 292, 311; zusammenfassend *Schmidt-Preuß*, 2005, S. 29.
[92] *Hammerstein*, MMR 2004, S. 224.
[93] *Welp*, 2000, S. 136.
[94] *Dorsch*, 2005, S. 33; *Welp*, 2000, S. 136.
[95] BVerfGE 30, S. 292, 311; BVerfGE 85, S. 329, 334; *Hammerstein*, MMR 2004, S. 223; *Welp*, 2000, S. 135.
[96] Gesetz über Fernmeldeanlagen v. 14. Januar 1928, RGBl. 1928 I, S. 8 ff.
[97] BGBl. 1989 I, S. 1455 v. 3. Juli 1989: Bekanntmachung der Neufassung des Gesetzes über Fernmeldeanlagen.
[98] *Seitz*, 2004, S. 149.
[99] *Bär*, MMR 2002, S. 358; *Seitz*, 2004, S. 149; vgl. auch *Wolter*, in: SK StPO, 2006, § 100g Rn. 1.

Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft in strafgerichtlichen Untersuchungen Auskunft über die Telekommunikation verlangen, wenn die Mitteilungen an den Beschuldigten gingen oder wenn Tatsachen vorlagen, aus denen zu schließen war, dass die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren. Dabei musste die Auskunft für die Untersuchung von Bedeutung sein. Gemäß § 28 FAG, der 1994[100] in das FAG eingefügt worden war, sollte das Gesetz insgesamt nach dem 31. Dezember 1997 außer Kraft treten.

§ 12 FAG war immer wieder Gegenstand verfassungsrechtlicher Kritik. Die mangelnde Bestimmtheit der Eingriffsvoraussetzungen wurde als bedenklich angesehen.[101] Die Regelung der Verkehrsdatenabfrage außerhalb der StPO wurde zudem als unzureichend empfunden. In einem Gesetzesentwurf der Bundesregierung von 1997 war deshalb der Vorschlag unterbreitet worden, den Auskunftsanspruch in einem neuen § 99a StPO zu regeln.[102] § 99a StPO-E machte bei Verdacht einer nicht mittels Endeinrichtung begangenen Straftat eine „Straftat von nicht unerheblicher Bedeutung" zur Voraussetzung.[103] Ansonsten war eine zulässige Auskunft über die „näheren Umstände der Telekommunikation" für jede Straftat im Falle der Erforderlichkeit der Auskunft für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten vorgesehen. Durch Artikel 2 Abs. 35 des Begleitgesetzes zum TKG (BegleitG)[104] wurde jedoch die Geltungsdauer der Regelung des § 12 FAG bis zum 31. Dezember 1999 verlängert, da ein Konsens im Hinblick auf eine Nachfolgeregelung nicht erzielt werden konnte. Die Verlängerung stand unter der Bedingung der Vorlage eines neuen Entwurfs zu § 99a StPO bis zum 30.4.1998 durch die Bundesregierung.[105] Dabei sollten insbesondere die Berufsgeheimnisse angemessen abgesichert werden. Nach ergebnislosem Verstreichen der Frist wurde die Geltung des § 12 FAG bis zum 31. Dezember 2001 ausgedehnt.[106] Gleichzeitig wurde Absatz 2 des § 12 FAG eingeführt, der §§ 100b VI und § 101 I Satz 1 StPO für entsprechend anwendbar erklärte und damit die Vernichtungs- und Benachrichtigungspflicht auf die Abfrage von Verkehrsdaten erstreckte.[107] Erst Ende 2001 entschloss sich der Gesetzgeber zu einer Neuregelung, die die besondere Ermittlungsmaßnahme der Verkehrsdatenabfrage systematisch in den strafprozessualen Regelungskontext der Normen über die Telekommunikationsüberwachung eingliedert. Dabei sollten die Anordnungsvoraussetzungen für den Auskunftsanspruch im Interesse wirksamen Grundrechtsschutzes maßvoll angehoben werden.[108] Die Nachfolgebestimmungen in Gestalt der §§ 100g, 100h StPO traten am 1. Januar 2002 in Kraft.[109]

Der Inhalt der Bestimmungen wurde gegenüber der Vorgängerregelung in mehreren Punkten verändert. Zum einen bedarf es nunmehr in Fällen der Eilanordnung der Auskunftserteilung (Gefahr im Verzug) durch die Staatsanwaltschaft einer Bestätigung der Eilmaßnahme innerhalb einer Frist von drei Tagen durch den Richter. Außerdem wird die Auskunftsanordnung auch über zukünftig gespeicherte Telekommunikationsverkehrsdaten zugelassen. Begründet wurde dies mit dem Interesse an einer wirksamen Strafrechtspflege.[110] Zudem wurden die Voraussetzungen der „Straftat von erheblicher Bedeutung" oder „mittels Endeinrichtung begangenen Straftat" in den Gesetzestext aufgenommen. Die Geltungsdauer der Regelungen wurde zunächst auf den 31. Dezember 2004 befristet. Bis zu diesem Zeitpunkt sollte ursprünglich eine Gesamtnovellierung der §§ 100a ff. StPO mit dem Ziel erfolgen, ein harmonisches System aller verdeckten Ermittlungsmaßnahmen zu schaffen und insbesondere für die Berücksichtigung der Zeugnisverweigerungsrechte ein geschlossenes Regelungskonzept vorzulegen.[111] Da die Gesamtnovelle Ende 2004 noch nicht realisiert war, wurde die Geltungsdauer der §§ 100g, 100h StPO noch einmal bis zum 31. Dezember 2007 verlängert.[112]

In seiner 132. Sitzung vom 21. Oktober 2004 forderte der Bundestag dann die Bundesregierung dazu auf, bis zum 30. Juni 2007 einen Erfahrungsbericht über die praktische Umsetzung des „Gesetzes zur Verlängerung der Geltungsdauer der §§ 100g, 100h StPO" und der §§ 100g, 100h StPO seit deren Einführung vorzulegen und dabei Anlass, Ergebnisse und die Anzahl der Betroffenen der Maßnahmen zu berücksichtigen.[113] Dieser Entschließungsantrag wurde vom Rechtsausschuss des Bundestages einstimmig angenommen. Der Antrag enthält sowohl den Auftrag, die bisherige Rechtswirklichkeit der Anwendung der genannten Rechtsnormen zu überprüfen, als auch die Aufforderung, ein Konzept über ihre zukünftige Verwendungspraxis zu erstellen.

Ein solcher Erfahrungsbericht kann nur auf der Grundlage einer systematischen, empirischen Untersuchung der Maßnahmen nach §§ 100g, 100h StPO erstellt werden. Hierfür hat das Bundesministerium der Justiz dem Max-Planck-Institut für ausländisches und internationales Strafrecht den Auftrag zur Durchführung einer An-

[100] BGBl. 1994 I, S. 2325, 2368: Artikel 5 Nr. 20 des Gesetzes zur Neuordnung des Postwesens und der Telekommunikation vom 14. September 1994.

[101] Bundestagsdrucksache 14/7008, S. 1 v. 1. Oktober 2001; Bundestagsdrucksache 14/7679, S. 1 v. 28. November 2001; *Wollweber*, NJW 2002, S. 1554.

[102] Bundesratsdrucksache 369/97; Bundestagsdrucksache 13/8016, S. 9 v. 23. Juni 1997.

[103] Bundesratsdrucksache 369/97, S. 13; Bundestagsdrucksache 13/8016, S. 9 v. 23. Juni 1997.

[104] BGBl. I 1997, S. 3108, 3118; Bundestagsdrucksache 13/8776, S. 27.

[105] Bundestagsdrucksache 13/8776, S. 32; *Bär*, MMR 2002, S. 359.

[106] BGBl. I 1999 Nr. 57, S. 2491, 2492: Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des FAG v. 20.12.1999, Artikel 4 Nr. 2.

[107] BGBl. I 1999 Nr. 57, S. 2491, 2492: Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des FAG v. 20. Dezember 1999, Artikel 4 Nr. 1.

[108] Bundestagsdrucksache 14/7679, S. 1.

[109] BGBl. I 2001 Nr. 73, S. 3879: Gesetz zur Änderung der StPO v. 20. Dezember 2001.

[110] Bundestagsdrucksache 14/7679, S. 2.

[111] Bundesratsdrucksache 702/01, S. 10, 11.

[112] BGBl. I 2004 Nr. 66, S. 3231: Gesetz zur Verlängerung der Geltungsdauer der §§ 100g, 100h StPO v. 9. Dezember 2004; Bundestagsdrucksache 15/3349, S. 1, 6.

[113] Bundestagsdrucksache 15/3971, S. 3f. (Beschlussempfehlung v. 20. Oktober 2004).

schlussstudie zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverkehrsdaten nach §§ 100g, 100h StPO“ erteilt. Die Ergebnisse dieser Studie sollen Aufschluss über die Anwendungspraxis der Verkehrsdatenabfrage, ihre Probleme und ihre Effizienz, auch in Kombination mit anderen Telekommunikationsüberwachungsmaßnahmen, geben.

II. Begriff der Verbindungs- bzw. Verkehrsdaten

Mit jedem Telekommunikationsvorgang fallen Verkehrsdaten an.[114] Bei der herkömmlichen analogen Übertragung gehen diese Daten mit der Beendigung der Verbindung verloren. Demgegenüber erzeugt die digitale Vermittlungstechnik für jede Kommunikation einen Datensatz, der zumindest kurzfristig gespeichert wird.[115] Während in § 100g StPO noch der Begriff „Verbindungsdaten“ verwendet wird, ist im Telekommunikationsgesetz (TKG) von „Verkehrsdaten“ die Rede. Mit beiden Begriffen sind dieselben Daten gemeint. Der Begriff der Verkehrsdaten ersetzt den bisherigen Begriff der Verbindungsdaten.[116]

Der Begriff der Verkehrsdaten wird in § 3 Nr. 30 TKG definiert. Danach sind Verkehrsdaten solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Detaillierte Informationen zum Inhalt des Verkehrsdatenbegriffs sind in § 100g III StPO und in § 96 I TKG enthalten. Gemäß § 100g III StPO sind Telekommunikationsverbindungsdaten im Falle einer Verbindung Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung, Beginn und Ende der Verbindung nach Datum und Uhrzeit, vom Kunden in Anspruch genommene Telekommunikationsdienstleistung sowie Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit. Diese Aufzählung orientiert sich an den früheren Vorschriften des TDSV[117] und erfasst damit diejenigen Verkehrsdaten, die grundsätzlich erhoben, verarbeitet und genutzt werden dürfen.[118] Nicht von § 100g StPO erfasst sind dagegen Teledienstenutzungsdaten.[119]

Unter dem Begriff Kennung versteht man insbesondere die IMEI-Nummer (International Mobile Equipment Identification = elektronische Gerätekennung von Mobiltelefonen, die im Rahmen der Telekommunikation übertragen wird) sowie die IP-Adressen von Computern, die einen Zugang zum Internet herstellen.[120] Bei den IP-Adressen ist zwischen dynamischen und statischen Adressen zu unterscheiden. Während eine statische IP-Adresse einem Nutzer dauerhaft zugewiesen ist, werden dynamische IP-Adressen für jede Verbindung, die den Zugang zum Internet herstellt, neu vergeben.[121] Die so genannte Standortkennung,[122] die den Ort des Mobilfunkgeräts bestimmt, wird ebenfalls registriert. Bei Mobiltelefonen wird zusätzlich die IMSI (International Mobile Subscriber Identity = die auf der SIM-Karte abgelegte Teilnehmeridentifikationsnummer) gespeichert.[123] Eine E-Mail-Adresse stellt ebenfalls eine Kennung dar.[124] Der Inhalt der Betreffzeile und die Bezeichnung etwaiger Anlagen zur E-Mail können dagegen nicht nach §§ 100g, 100h StPO herausverlangt werden, da sie zum Inhalt der Kommunikation gehören und damit nur § 100a StPO unterfallen.[125]

Die in § 100g III Nr. 1 StPO enthaltene Auskunftspflicht erfasst nur Daten, die „im Fall einer Verbindung“ entstanden sind. Ausgeschlossen sind daher Daten, die im Rahmen eines erfolglosen Versuches einer Kommunikation anfallen.[126] Besondere Aufmerksamkeit wird durch den Stand-by-Betrieb eines Mobilfunkgeräts entstehenden („geografischen“) Daten zuteil.[127] Jedes Mobilfunknetz ist in Funkzellen, d. h. geographisch umschriebene Bereiche, unterteilt, in denen eine funktechnische Versorgung stattfindet.[128] Ein auf Stand-by-Betrieb gestelltes Mobiltelefon meldet sich in der Funkzelle an, in der es sich befindet,[129] und kann daher lokalisiert werden.[130] Auf der Grundlage der geografischen Daten kann ohne weiteres ein (zeitnahes) Bewegungsbild erstellt werden. Ein Bundesgerichtshof-Ermittlungsrichterbeschluss hat im Jahr 2001 angenommen, dass §§ 100a, 100b StPO die Überwachung von Mobiltelefonen im Bereitschaftsmodus erlauben.[131] Danach sind die Netzbetreiber verpflichtet, die zur Standortbestimmung des Mobiltelefons erforderlichen geographischen Daten der betroffenen Funkzellen unabhängig von der Nutzung des Mobiltelefons zur Kommunikation herauszugeben.[132] Nach der Gesetzesbegründung zu §§ 100g, 100h StPO sind jedoch Auskünfte über Aktivmeldungen von Mobiltelefonen in „stand-by“-Funktion im Rahmen der Verkehrsdatenabfrage ausgeschlossen.[133] Auf eine Erweiterung der §§ 100g, 100h StPO um Stand-by generierte geografische Daten wurde wegen der hierdurch bedingten Vertiefung des Eingriffs verzichtet.[134] Die eindeutige Entscheidung für

---

114 *Nack*, in: Karlsruher Kommentar, 2003, § 100a Rn. 13.
115 *Nack*, in: Karlsruher Kommentar, 2003, § 100a Rn. 13.
116 *Piepenbrock,* in: Beck'scher TKG-Kommentar, § 3 Rn. 66.
117 Aufgehoben durch § 152 II TKG vom 25. Juni 2004 (BGBl. I 2004 Nr. 29, S. 1190, 1242).
118 Bundestagsdrucksache 14/7008, S. 7; *Meyer-Goßner*, § 100g Rn. 4; *Piepenbrock*, in: Beck'scher TKG-Kommentar, 2006, § 3 Rn. 66.
119 *Nack*, in: Karlsruher Kommentar, 2003, § 100g Rn. 8.
120 Bundestagsdrucksache 14/7008, S. 7; *Meyer-Goßner*, 2006, § 100g Rn. 4; *Pfeiffer*, 2005, § 100g Rn. 6.
121 *Königshofen,* in: BKA (Hrsg.), 2004, S. 75.
122 *Nack*, in: Karlsruher Kommentar, 2003, § 100a Rn. 13.
123 *Nack*, in: Karlsruher Kommentar, 2003, § 100a Rn. 13.
124 *Wohlers/Demko*, StV 2003, S. 243.
125 *Seitz*, 2004, S. 163.
126 *Welp*, GA 2002, S. 554; *Wohlers/Demko*, StV 2003, S. 243.
127 *Demko*, NStZ 2004, S. 57ff.
128 *Artkämper*, Kriminalistik 1998, S. 202; vgl. auch *Danckwerts*, CR 2002, S. 540.
129 *Artkämper*, Kriminalistik 1998, S. 202; *Demko,* NStZ 2004, S. 57; *Welp,* GA 2002, S. 553; vgl. auch *Deckers*, StraFo 2002, S. 112.
130 *Weßlau*, ZStW 113 (2001), S. 688.
131 Ermittlungsrichter des BGH, Beschluss v. 21. Februar 2001 § 2 BGs 42/2001; BGH NJW 2001, S. 1587; BGH NStZ 2002, S. 103.
132 Ermittlungsrichter des BGH, Beschluss v. 21. Februar 2001 § 2 BGs 42/2001, S. 3.
133 Bundestagsdrucksache 14/7008, S. 7.
134 Bundesratsdrucksache 702/01, S. 8; *Keller*, Die Polizei 2005, S. 112; *Meyer-Goßner*, 2006, § 100g Rn. 5.

die Beschränkung auf den Fall einer Verbindung in § 100g III StPO schließt aus, dass Stand-by generierte geografische Daten in den Geltungsbereich der Ermittlungsmaßnahme der Verkehrsdatenauskunft fallen.[135] Die geografischen Daten haben freilich aus der Perspektive von Ermittlungsmaßnahmen – unabhängig, ob sie außerhalb oder anlässlich von Kommunikationsvorgängen zustande kommen – auch die Funktion der Observierung des Mobiltelefons (eingeschränkt auf die Beobachtung von räumlichen Bewegungen und der Vornahme von Kommunikation).[136] Die aus Kommunikationstechnologie und elektronischer Datenverarbeitung resultierenden Informationen sind multi-funktional und können in jeweils angepasster Art und Weise in die Ermittlungsmaßnahmen der Observation, der Telekommunikationsüberwachung und der Rasterfahndung eingeordnet werden. Dies gilt im Übrigen auch für die Datensysteme des elektronischen Zahlungsverkehrs bzw. der Kreditkartenorganisationen, die nicht nur Informationen über wirtschaftliche Transaktionen, sondern Bewegungsbilder und Handlungsmuster abbilden.

Der Anspruch auf Auskunftserteilung beschränkt sich auf solche Daten, die seitens der Diensteanbieter auf Grund bestehender Regelungen zulässigerweise erhoben und gespeichert werden.[137] Das sind nach § 96 II TKG nur solche Daten, die zum Aufbau von Verbindungen, zur Entgeltermittlung und Entgeltabrechnung, zur Erstellung eines Einzelverbindungsnachweises, zur Erkennung bzw. Beseitigung von Störungen von Telekommunikationsleistungen oder von Missbrauch von Telekommunikationsdiensten, benötigt werden.

Von den Verkehrsdaten sind die Bestandsdaten zu unterscheiden. Bestandsdaten sind nach § 3 Nr. 3 TKG Daten eines Teilnehmers, die zur Begründung, inhaltlichen Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Erfasst werden dabei insbesondere Name und Anschrift des Kunden.[138] Dabei entstehen Unsicherheiten in der Grenzziehung zwischen Verkehrsdaten und Bestandsdaten insbesondere bei dynamischen IP-Adressen. Hier stellt sich die Frage, ob Name und Anschrift der hinter einer dynamischen IP-Adresse stehenden Person zu den Verkehrs- oder zu den Bestandsdaten zählen. Während bei Personendaten hinter statischen IP-Adressen Einigkeit darüber besteht, dass es sich um Bestandsdaten handelt[139], ist die Zuordnung bei dynamischen IP-Adressen sowohl in Rechtsprechung als auch in Literatur und ferner zwischen den Beteiligten der Verkehrsdatenabfrage umstritten.[140] Die Betrachtung einer dynamischen IP-Adresse als Bestandsdatum stützt sich im Wesentlichen auf den Gedanken, dass mit dem Wissen über die Kennung eines an einem Telekommunikationsvorgang beteiligten Endgerätenutzers auch der betreffende Anschlussinhaber eindeutig und unverwechselbar individualisiert ist.[141] Da der Kommunikationsvorgang selbst bereits bekannt ist, so wird nunmehr angenommen, komme es nur mehr auf die Konkretisierung der Identität durch Namen und Anschrift an.[142] Tatsächlich sprechen die technischen und betrieblichen Rahmenbedingungen zunächst dafür, dynamische und statische IP-Adressen gleich zu behandeln. Der Bedarf an Nutzung dynamischer Adressen folgt aus einer begrenzten Anzahl von Zugangsprovidern insgesamt zur Verfügung stehenden Adressen. Hierdurch wird erst eine Differenzierung in der praktischen Nutzung der Kommunikationsverbindungen erzeugt, die sich jedoch im normativen Gefüge der §§ 113 I Satz 1 TKG, 100g StPO nicht wiederfindet. Dem steht die Argumentation gegenüber, dass allein durch die Kombination einer dynamischen IP-Adresse mit Verkehrsdaten eben noch keinen Aufschluss über eine einem bestimmten Anschluss zuordnungsfähige Kommunikation gegeben wird. Erst die nachträgliche Herstellung der Zusammenhänge zwischen dynamischer IP-Adresse, Verkehrsdaten und Bestandsdaten erlauben demnach einen Zugriff auf die in den Schutzbereich des Artikel 10 GG fallenden Kommunikationsumstände.[143] An den die Kommunikationsumstände begründenden Verkehrsdaten sind zwar Strafverfolgungsbehörden nicht primär interessiert, doch ändert dies nichts daran, dass die Bestandsdaten in diesem Fall mit den Verkehrsdaten so vermengt sind, dass nur IP-Adresse, Verbindung und Bestandsdaten eine (umfassende) Information ergeben, aus der sich dann wiederum eindeutige Informationsbruchstücke (wie Name und Adresse einer Person) lösen lassen.[144]

III. Delikte und Verdachtsgrad

Gemäß § 100g I Satz 1 StPO ist Voraussetzung für eine Auskunftserteilung der Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von erheblicher Bedeutung, insbesondere eine der in § 100a Satz 1 StPO genannten

[135] Überzeugend *Demko,* NStZ 2004, S. 57ff; vgl. im Übrigen *Hoeren*, wistra 2005, S. 3; *Meyer-Goßner,* 2006, § 100g Rn. 4; *Piepenbrock,* in: Beck'scher TKG-Kommentar, 2006, § 3 Rn. 66; *Wohlers/Demko,* StV 2003, S. 242; *Keller,* Die Polizei, 2005, S. 113.

[136] *Gercke*, Bürgerrechte & Polizei/CILIP 71(2002), S. 24; *Demko,* NStZ 2004, S. 57f.

[137] *Hoeren*, wistra 2005, S. 3; Meyer-Goßner, 2006, § 100g Rn. 4; Piepenbrock, in: Beck´scher TKG-Kommentar, 2006, § 3 Rn. 66; *Wohlers/Demko*, StV 2003, S. 242.

[138] *Nack*, in: Karlsruher Kommentar, 2003, § 100a Rn. 16.

[139] LG Hamburg, MMR 2005, S. 711, 712; *Sankol,* MMR 2006, S. 363.

[140] Bundestagsdrucksache 14/7008, S. 7; LG Hamburg, MMR 2005, S. 711; LG Stuttgart, NJW 2005, S. 614; LG Stuttgart, DuD 2005, S. 232; LG Würzburg, NStZ-RR 2006, S. 46; *Meyer-Goßner*, 2006, § 100g Rn. 4; *Pfeiffer*, 2005, § 100g Rn. 6; *Sankol*, JuS 2006, S. 702; *Sankol*, MMR 2006, S. 365; für die Einstufung als Verkehrsdatum LG Bonn, DuD 2004, S. 628; LG Ulm, CR 2004, S. 35; *Bock*, in: Beck'scher TKG-Kommentar, 2006, § 113 Rn. 24; *Hoeren*, 2004, Rn. 192; *Nack*, in: Karlsruher Kommentar, 2003, § 100a Rn. 13.

[141] LG Hamburg, MMR 2005, S. 711, 712; LG Stuttgart, DuD 2005, S. 232, 233; LG Stuttgart, NStZ 2005, S. 285, 286; LG Würzburg, NStZ-RR 2006, S. 46, 47.

[142] LG Würzburg, NStZ-RR 2006, S. 46, 47; LG Stuttgart, NStZ 2005, S. 285, 286; so auch *Sankol,* MMR 2006, S. 364.

[143] *Schramm*, DuD 2006, S. 787.

[144] LG Bonn, DuD 2004, S. 628, 629; *Bock*, in: Beck'scher TKG-Kommentar, 2006, § 113 Rn. 24; *Köbele*, DuD 2004, S. 609; *Königshofen,* in: BKA (Hrsg.), 2004, S. 75.

Straftaten, oder eine Straftat mittels einer Endeinrichtung begangen hat. Dabei genügt wie bei anderen verdeckten Ermittlungsmaßnahmen ein sogenannter gesteigerter Anfangstatverdacht,[145] der sich aus Umständen ergibt, die nach der Lebenserfahrung in erheblichem Maße darauf hindeuten, dass jemand als Täter oder Teilnehmer eine Katalogtat oder eine andere unter § 100g I StPO subsumierbare Straftat begangen hat; der Tatverdacht muss weder dringend noch vollständig konkretisiert sein.[146]

1. Straftat von erheblicher Bedeutung

Weitere Voraussetzung ist das Vorliegen einer Straftat von erheblicher Bedeutung. Die Straftat muss mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.[147] Für die Bestimmung der erheblichen Bedeutung ist auf den konkreten Einzelfall abzustellen.[148] Konkretisiert wird der unbestimmte Rechtsbegriff „Straftat von erheblicher Bedeutung“ durch einen (nicht ausschließenden) Verweis auf den Straftatenkatalog des § 100a Satz 1 StPO.[149] Nach dem Willen des Gesetzgebers sollen durch den Bezug auf die in § 100a StPO genannten Straftaten die Anordnungsvoraussetzungen des Auskunftsanspruchs weiter präzisiert und „die für eine sachgerechte Anwendung der Vorschrift erforderliche Flexibilität“ erhalten werden.[150] Diese Form der Präzisierung war bei Einführung der Vorschriften umstritten. Nach den Vorstellungen des Bundesrats sollte der Bezug auf die Katalogdelikte der Telekommunikationsüberwachung in § 100g I Satz 1 StPO entfallen, da der Verweis auf § 100a StPO im Ergebnis zu einer „kontraproduktiven Einschränkung“ führe und eine flexible Anwendung unnötig erschwere. Durch das Kriterium der Straftaten von erheblicher Bedeutung werde eine durch die Tatschwere geleitete Begrenzung der Anwendung ausreichend gewährleistet.[151] Dabei wird auch auf eine im Vergleich zur Telekommunikationsüberwachung nach §100a StPO geringere Eingriffstiefe der Verkehrsdatenabfrage abgestellt.[152]

Wegen Unbestimmtheit hat der Begriff der „Straftat von erheblicher Bedeutung“ freilich teilweise auch Kritik auf sich gezogen.[153] Danach resultiert aus dem Verweis auf den Katalog des § 100a StPO die Gefahr ausgedehnter Wertungsspielräume.[154] Hinzu tritt eine kritische Betrachtung bereits des Katalogs des § 100a StPO, dem vereinzelt ein Potential für allgemeine Aussagen über den geforderten Deliktscharakter abgesprochen wird.[155] Jedoch wird auch eine Übertragung des § 100a-Katalogs auf § 100g StPO befürwortet.[156] Das Bundesverfassungsgericht hat indessen die Verwendung des Begriffs „Straftat von erheblicher Bedeutung“ wiederholt nicht beanstandet und konkrete Vorgaben für die Ausfüllung des Begriffs aufgestellt [157].

2. Straftat, die mittels einer Endeinrichtung begangen wurde

§ 100g I Satz 1 StPO erlaubt die Abfrage der Verkehrsdaten neben Straftaten von erheblicher Bedeutung auch bei Delikten, die mittels Endeinrichtung begangen wurden. Der Verweis auf die Definition des Begriffes der Endeinrichtung in § 3 Nr. 3 TKG a. F. ist freilich überarbeitungsbedürftig, da in § 3 Nr. 3 TKG n. F. heute der Begriff der Bestandsdaten festgelegt wird.

Straftaten werden mittels einer Endeinrichtung begangen, wenn das Telefon, das Faxgerät oder der Internetzugang des Computers eingesetzt werden.[158] Denkbar sind hierbei zum einen die typischen Internetstraftaten wie das Ausspähen von Daten, Datenmanipulation und Urheberrechtsverletzungen. Daneben kommt die Verbreitung pornographischer Bilder oder extremistischer Schriften in Betracht. Ferner fallen Betrugshandlungen bei Internetauktionen oder mittels Telekommunikation begangene Beleidigungen, Bedrohungen, Stalkingstraftaten oder Erpressungen unter die Fallgruppe „Endeinrichtungen“ des § 100g I StPO. In diesen Fällen ist die Verkehrsdatenabfrage selbstverständlich ein zentrales Instrument der Sachverhaltsaufklärung und Beweissicherung.[159]

Eine bloße Randbedeutung kommt der Frage zu, ob auch die Straftaten, die mittels Endeinrichtung begangen worden sind, von erheblicher Bedeutung sein müssen. Nach vorherrschender Meinung in Rechtsprechung und Literatur bedarf es hier freilich keiner erheblichen Bedeutung.[160] Denn der Gesetzestext stellt eindeutig fest, dass es sich um alternative Möglichkeiten handelt.[161] Diese Auslegung entspricht dem Willen des Gesetzgebers, dem

---

[145] *Meyer-Goßner*, 2006, § 100g Rn. 6; vgl. auch Bundestagsdrucksache 14/7008, S. 6.
[146] *Nack*, in: Karlsruher Kommentar, 2003, § 100a Rn. 22; *Seitz*, 2004, S. 158.
[147] BVerfGE 103, S. 21, 34; Bundestagsdrucksache 13/10791, S. 5; *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 13; *Seitz*, 2004, S. 153.
[148] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 13; *Seitz*, 2004, S. 153.
[149] Vgl. BGH NStZ 2001, S. 598; *Nack*, in: Karlsruher Kommentar, 2003, § 100g Rn. 4.
[150] Bundestagsdrucksache 14/7008, S. 6; Bundestagsdrucksache 14/7258, S. 4.
[151] Bundestagsdrucksache 14/7258, S. 1.
[152] Bundestagsdrucksache 14/7258, S. 1.
[153] *Welp*, GA 2002, S. 539; *Wohlers/Demko*, StV 2003, S. 245.
[154] *Wohlers/Demko*, StV 2003, S. 245.
[155] *Welp*, GA 2002, S. 540.
[156] *Wohlers/Demko*, StV 2003, S. 245; vgl. auch *Welp,* GA 2002, S. 538.
[157] BVerfGE 103, S. 21ff, S. 34; 109, S. 279ff, S. 344.
[158] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 14; *Meyer-Goßner*, 2006, § 100g Rn. 6; *Welp*, GA 2002, S. 540.
[159] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 14.
[160] LG Ulm, Anmerkung *Bär*, MMR 2004, S. 187; LG Wuppertal, MMR 2002, S. 560; *Bock*, in: Beck´scher TKG-Kommentar, 2006, § 88 Rn. 37; *Lüken*, Die Polizei 2002, S. 224; *Welp*, GA 2002, S. 540.
[161] *Nack*, in: Karlsruher Kommentar, 2003, § 100g Rn. 4; *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 14; *Seitz*, 2004, S. 152; *Welp*, GA 2002, S. 540.

es auch auf die Aufklärbarkeit weniger schwerwiegender Delikte wie z. B. beleidigender Anrufe ging, wenn für die Untersuchungen im Wesentlichen nur Verkehrsdaten erfolgversprechende Anhaltspunkte bieten.[162] Wenn gleichwohl die Gesetzesformulierung als „sprachlich nicht gelungen[163]„ als „etwas unklar formuliert[164]„ oder als „grammatikalisch unvollständig[165]„ bezeichnet wird[166], dann lässt sich dies als Aufforderung an den Gesetzgeber interpretieren, eine sprachliche Überarbeitung einzuleiten.

IV. Arten der Verkehrsdatenabfrage

Die Verkehrsdatenabfrage bezieht sich auf verschiedene Typen von Verkehrsdaten. Einerseits kann sich die Abfrage auf bereits entstandene Daten beziehen und auf einen Zeitraum in der Vergangenheit erstrecken. Die Abfrage von Verkehrsdaten, die bereits entstanden sind, ist in § 100g I Satz 1 StPO geregelt, diejenige von in der Zukunft entstehenden Daten ist in § 100g I Satz 3 StPO angesprochen.

Zukünftige Verkehrsdaten werden sowohl von § 100a StPO als auch von § 100g StPO erfasst.[167] Im Rahmen der Telekommunikationsüberwachung werden Gesprächsprotokolle erstellt, aus denen sich die Verkehrsdaten, einschließlich der geografischen Daten, ergeben.[168] Jedoch kann nicht davon ausgegangen werden, dass mit der Ausdehnung der Verkehrsdatenabfrage gemäß §§ 100g, 100h StPO auch auf zukünftige Daten (im Gegensatz zu § 12 FAG) §§ 100a, 100b StPO eine Anpassung dahingehend erfahren hätten, dass nur noch zukünftige Inhaltsdaten und nicht mehr Verkehrsdaten davon erfasst würden.[169] Mit der Überwachung der Telekommunikation werden auch Verkehrs- und geografische Daten erhoben. Im Übrigen sind die Anforderungen an die Telekommunikationsüberwachung im Vergleich zur Abfrage von Verkehrsdaten immer noch erhöht (wenngleich angeglichen), sodass es auch aus dieser Perspektive keinen Sinn machte, die Verkehrsdaten aus der Anordnung der Telekommunikationsüberwachung herauszulösen.

Weitere Anwendungsbereiche sind die Zielwahlsuche und die Funkzellenabfrage. Gemäß § 100g II Satz 1 StPO darf die Erteilung einer Auskunft darüber, ob von einem Telekommunikationsanschluss Verbindungen zu den in § 100g I Satz 2 StPO genannten Personen hergestellt worden sind, angeordnet werden (Zielwahlsuche). Insoweit sollen solche noch unbekannte Anschlussnummern ermittelt werden, von denen Telekommunikationsverbindungen zu einem Anschluss hergestellt worden sind.[170] Im Rahmen der Ermittlung der herauszugebenden Verkehrsdaten müssen deshalb die Telekommunikationsverbindungen aller Kunden einbezogen und, ähnlich einer Rasterfahndung, auf die Herstellung von Verbindungen zu dem in der Anordnung angegebenen Anschluss abgeglichen werden.[171] Dieser Verarbeitungsschritt ist notwendig, weil Verkehrsdaten nur zu Abrechnungszwecken gespeichert werden.[172] Da der Kommunikationspartner des Anschlussinhabers aber dem Anbieter (abgesehen von Anrufen aus dem Ausland) kein Entgelt schuldet, werden die eingehenden Verkehrsdaten nicht gespeichert.[173] Die Suchläufe werden von den großen Anbietern täglich für mehrere Anfragen durchgeführt.[174] Der Abgleich umfasst damit alle Verkehrsdaten des deutschen Telekommunikationsverkehrs mit der Folge, dass diese Daten einer „permanenten strafprozessualen Kontrolle“ unterliegen[175]. Wegen der Reichweite der Zielwahlsuche hat der Gesetzgeber eine besondere Subsidiaritätsklausel eingefügt. Das Bundesverfassungsgericht[176] hat allerdings angenommen, dass ein Eingriff in Rechte Dritter nicht vorliege, weil der Zugriff auf deren Daten nur flüchtig sei. Denn alle nicht betroffenen Telekommunikationsteilnehmer werden unmittelbar aus dem Verfahren ausgeschieden und eine Speicherung von Daten erfolgt nur im Falle von Treffern. Aus einer anderen Perspektive werden sodann die aktive Rolle der Telekommunikationsunternehmen an den Ermittlungen und das besondere Maß ihrer Verpflichtung zur Durchführung von Ermittlungsmaßnahmen betont [177]

Die Funkzellenabfrage wird durch § 100g i. V. m. § 100h I Satz 2 StPO erlaubt[178]. Sie ermöglicht im Falle einer Straftat von erheblicher Bedeutung den Zugriff auf Verkehrsdaten dann, wenn eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation vorliegt. Die Funkzellenabfrage dient dem Versuch der Identifizierung noch unbekannter Täter und bezieht sich auf die Daten aller Mobilfunktelefonate, die während eines bestimmten Zeitraums in einer bestimmten Region geführt wurden (vgl. hierzu weiter oben 2., A. I. 1.).[179] Die Regelung der Funkzellenabfrage in der „Formvorschrift“ des § 100h StPO wird als unsystematisch platziert eingestuft.[180]

---

[162] Bundestagsdrucksache 14/7008, S. 7; Bundestagsdrucksache 14/7679, S. 1; *Bär*, MMR 2002, S. 361.
[163] *Seitz*, 2004, S. 152.
[164] LG Ulm, Anmerkung *Bär*, MMR 2004, S. 187.
[165] LG Wuppertal, MMR 2002, S. 560.
[166] AG Ulm, MMR 2003, S. 55.
[167] *Demko*, NStZ 2004, S. 59; *Günther*, in: BKA (Hrsg.), 2004, S. 65; *Schäfer*, in: Löwe-Rosenberg, 2004, § 100a Rn. 49.
[168] *Demko*, NStZ 2004, S. 59.
[169] So wohl *Wolter*, in: SK StPO, 2006, § 100g Rn. 6, mit dem Hinweis, § 100a StPO stelle nach der Einführung des § 100g StPO ein „aliud“ dar; überzeugend Demko, NStZ 2004, S. 59.
[170] *Bär*, MMR 2002, S. 361; *Meyer-Goßner*, 2006, § 100g Rn. 11.
[171] Bundestagsdrucksache 14/7008, S. 7; *Bär*, MMR 2002, S. 361; *Wollweber*, NJW 2002, S. 1554.
[172] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 27; *Wohlers/Demko*, StV 2003, S. 247.
[173] *Welp*, GA 2002, S. 542.
[174] *Welp*, GA 2002, S. 543.
[175] *Welp*, GA 2002, S. 543.
[176] BVerfG NJW 2003, S. 1787, 1793.
[177] *Wollweber*, NJW 2002, S. 1554.
[178] Bundestagsdrucksache 14/7679, S. 8; *Nack*, in: Karlsruher Kommentar, 2003, § 100h Rn. 4; *Wolter*, in: SK StPO, 2006, § 100h Rn.1.
[179] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 19.
[180] *Danckwerts*, CR 2002, S. 541; *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 28.

Von der Funkzellenabfrage ist die sog. *Standortbestimmung* zu unterscheiden. Hier ist die Funkzelle oder der räumliche Bereich, in dem sich der Beschuldigte aufgehalten hat, unbekannt. Mittels der Standortbestimmung oder Geodatenfeststellung soll der Aufenthaltsort des Verdächtigen, bzw. der Ort, an dem sich das auf ihn zugelassene Mobiltelefon befindet, festgestellt werden. Diese Standortbestimmung wird aufgrund der Definition der Verkehrsdaten in § 100g III StPO mit dem Begriff „Standortkennung" bezeichnet.

Für die Funkzellenabfrage gilt eine spezielle Subsidiaritätsklausel. Die Anforderungen an die Abfrage werden durch das Merkmal „Straftat von erheblicher Bedeutung" erhöht. Die Funkzellenabfrage erfasst eine zunächst unbekannte Anzahl von Telekommunikationsteilnehmern.[181] Im Unterschied zur Zielwahlsuche bleibt die Erfassung allerdings nicht flüchtig, denn die Verkehrsdaten der Telekommunikation, die im in der Anordnung genannten Raum und während des bezeichneten Zeitraums geführt worden ist, werden an die Strafverfolgungsbehörden weiter gegeben und dort zum Ausgangspunkt weiterer Ermittlungen (vgl. hierzu weiter oben 2. A. I. 1.).[182]

In Tabelle 1 sind die einzelnen Arten der Verkehrsdatenabfrage und dadurch betroffene Grundrechte zusammenfassend dargestellt.

[181] *Wohlers/Demko*, StV 2003, S. 247.
[182] Vgl. hierzu *Danckwerts*, CR 2002, S. 542.

Tabelle 1

Arten der Verkehrsdatenabfrage

Art der Abfrage	Kriminalistische Bedeutung	Grundrechtsbetroffenheit
Abfrage vorhandener Daten	Bereits vorhandene Daten werden abgefragt, um z. B. festzustellen, mit wem das Opfer eines Tötungsdelikts im Zeitraum vor der Tat Kontakt hatte. Es handelt sich um eine Art Einzelverbindungsnachweis über die von dem Anschluss aus geführten Telefonate.	Durch die Abfrage vorhandener Daten sind die Grundrechte des Anschlussinhabers sowie die Rechte der Personen betroffen, mit denen der Anschlussinhaber telefoniert hat.
Abfrage zukünftiger Daten	Zukünftige Verkehrsdaten enthalten Informationen über aktuelle Kontakte, beispw. in Fällen der Transaktions- oder Netzwerkkriminalität (Täterverbindungen). Wie bei einer Telekommunikationsüberwachung werden hier regelmäßig Daten vom Provider an die Polizei geliefert.	Auch bei zukünftigen Verkehrsdaten sind Grundrechte des Anschlussinhabers und der übrigen an den Gesprächen Beteiligten tangiert. Die Abfrage der Daten gleicht hier von der Vorgehensweise her der Telekommunikationsüberwachung.
Zielwahlsuche	Anhand der Zielwahlsuche kann die Rufnummer eines unbekannten Anrufers identifiziert werden. Die abgehenden Daten von allen Rufnummern zu einer konkreten Rufnummer werden abgefragt.	Die Zielwahlsuche gleicht einer Rasterfahndung und überprüft alle Telekommunikationsteilnehmer auf Verbindungen zu einem bezeichneten Anschluss. Der Zugriff bleibt jedoch flüchtig, da Verkehrsdaten nur für Treffer gespeichert werden[183]
Funkzellenabfrage	Identifizierung unbekannter Täter: Mittels Funkzellenabfrage werden alle Ruf-/IMEI-Nummern, die innerhalb eines bestimmten Bereichs aktiv geworden sind, abgefragt.	Alle Personen, die sich in die abgefragte Funkzelle eingewählt haben, sind von der Abfrage der Daten betroffen.
Standortabfrage	Die Standortabfrage dient der Feststellung, an welchem Ort sich eine Person zu einer bestimmten Zeit aufgehalten hat.	Anhand der Standortabfrage kann ein Bewegungsbild über eine Person erstellt werden.

[183] Siehe oben Fn. 68

V. Subsidiarität

Neben dem allgemeinen Grundsatz der Verhältnismäßigkeit, der in § 100g I Satz 1 StPO durch das Wort „erforderlich" zum Ausdruck kommt, sind zwei ausdrückliche Subsidiaritätsklauseln in den Gesetzestext eingefügt worden.

1. Verhältnismäßigkeitsgrundsatz in § 100g I Satz 1 StPO

Wie jedes staatliche Handeln unterliegt auch die Auskunftserteilung dem Grundsatz der Verhältnismäßigkeit. Gemäß § 100g I Satz 1 StPO besteht ein Auskunftsanspruch nur, soweit die Auskunft für die Untersuchung erforderlich ist. Erforderlich i. S. d. § 100g I Satz 1 StPO ist eine Auskunft, wenn kein milderes Mittel zur Verfügung steht, um das jeweilige Ziel der Ermittlungsmaßnahme zu erreichen.[184] So soll beispielsweise die Einrichtung einer Fangschaltung dem Auskunftsverlangen vorgehen, falls diese zur Aufklärung ausreicht.[185] Ungeachtet der vom Gesetz vorgesehenen speziellen Eingriffsvoraussetzungen (Deliktskatalog, Erheblichkeit der Straftat, bestimmte Tatsachen für die Verdachtsannahme, Subsidiaritätsklausel bei der Zielwahlsuche nach § 100g II StPO und bei der Funkzellenabfrage nach § 100h I Satz 2 StPO) ist dann in jedem Einzelfall zu prüfen, ob der Grad des Tatverdachts und das Gewicht der Straftat oder der Teilnahmehandlung die Verhältnismäßigkeit der Maßnahme trägt.[186] In die Abwägung ist auch – darauf weist das Bundesverfassungsgericht[187] hin – die Frage einzubeziehen, welche Streubreite Eingriffe in Verkehrsdaten haben. Dabei ist der objektiv-rechtliche Gehalt des Fernmeldegeheimnisses in Form der Vertraulichkeit der Telekommunikation in ihrer gesamtgesellschaftlichen Bedeutung zu berücksichtigen. Kritisch wird hervorgehoben dass die Auskunftserteilung in der Praxis zu schnell und ohne Prüfung etwaiger Alternativmaßnahmen angeordnet wird.[188] Betont werden schließlich die Entwicklung der Kommunikationsüberwachung zu einer standardmäßigen Ermittlungsmaßnahme und der Wandel von „ultima ratio" Maßnahme zu einem „prima ratio" Instrument [189].

2. Subsidiaritätsklausel des § 100g II StPO (Zielwahlsuche)

Gemäß § 100g II StPO darf die Auskunftserteilung darüber, ob von einem Telekommunikationsanschluss Verbindungen zu den in § 100g I Satz 2 StPO genannten Personen hergestellt worden sind (Zielwahlsuche), nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre[190]. Die Einführung der Subsidiaritätsklausel im Rahmen der Zielwahlsuche als zusätzliche Eingriffsschwelle ist wegen der Herausgabe der Telekommunikationsverkehrsdaten Unverdächtiger und des einer Rasterfahndung vergleichbaren Vorgehens begründet.[191] Darüber hinaus erfasst jedenfalls der manuell (und weitgehend ohne Speicherung bzw. Eingriff) vorgenommene Abgleich alle Verkehrsdaten der deutschen Telekommunikation.[192] Ob der Subsidiaritätsgrundsatz in allen Fällen genügt, verhältnismäßige Entscheidungen sicher zu stellen,[193] wird zum Teil bezweifelt.[194] Begründet wird dies mit der Annahme fehlender praktischer Wirkungen, die aus der (plausiblen) Überzeugung resultiert, die Zielwahlsuche sei wohl (insbesondere unter Kostengesichtspunkten) immer die effektivste Maßnahme.[195] Damit dürfte eine Tendenz zur Entscheidung für das Vorliegen des Merkmals „wesentlicher" Erschwernis der Ermittlungen einhergehen.

3. Subsidiaritätsklausel des § 100h I Satz 2 StPO (Funkzellenabfrage)

Ein weiterer spezifischer Subsidiaritätsgrundsatz findet sich in § 100h I Satz 2 StPO. Ausgangspunkt ist hier die Pflicht, den Antragsbetroffenen genau zu identifizieren. Deshalb muss die Anordnung gemäß § 100h I Satz 1 StPO den Namen und die Anschrift des Betroffenen, gegen den sie sich richtet, sowie die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten. Nach § 100h I Satz 2 StPO genügt jedoch im Falle eines noch nicht identifizierten Tatverdächtigen oder Nachrichtenmittlers sowie im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, über die Auskunft erteilt werden soll (Funkzellenabfrage). Mit der Funkzellenabfrage werden die in einem bestimmten Zeitraum entstandenen Verkehrsdaten aller Mobilfunktelefonate in einer oder mehreren Funkzellen übermittelt. Dies führt auch zur Erfassung und Abgabe der Verkehrsdaten unbeteiligter Dritter, die allein deshalb in den Wirkungskreis von Ermittlungsmaßnahmen geraten und demnach auch einem generellen Tatverdacht ausgesetzt werden[196], weil sie zu einer bestimmten Zeit in einer bestimmten Funkzelle ein Mobiltelefon benutzt haben. Die Subsidiaritätsklausel des § 100h I Satz 2 StPO dient ebenso wie bei der Zielwahlsuche der Verstärkung des Grundrechtsschutzes anlässlich einer breitflächig angreifenden Ermittlungsmaßnahme.

---

[184] *Seitz*, 2004, S. 159.
[185] *Meyer-Goßner*, 2006, § 100g Rn. 7; *Sankol*, JuS 2006, S. 702; *Wolter*, in: SK StPO, 2006, § 100g Rn. 15.
[186] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 19.
[187] BVerfG NJW 2003, S. 1787, 1791 (Urteil v. 12. März 2003, 1 BvR 330/96 und 1 BvR 348/99).
[188] *Dix*, Kriminalistik 2004, S. 82; vgl. zu den Anforderungen auch BVerfG NJW 2003, S. 1787, 1792.
[189] *Dix*, Kriminalistik 2004, S. 83.
[190] LG Ulm, Beschluss v. 4. November 2004, 2 Qs 2099/04.
[191] *Meyer-Goßner*, 2006, § 100g Rn. 11; *Wollweber*, NJW 2002, S. 1554.
[192] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 27; *Welp*, GA 2002, S. 545.
[193] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 27.
[194] *Welp*, GA 2002, S. 546; *Weßlau*, ZStW 113, S. 693 ff; *Wohlers/Demko*, StV 2003, S. 247.
[195] *Welp*, GA 2002, S. 546; *Wohlers/Demko*, StV 2003, S. 247.
[196] *Backes/Gusy*, StV 2003, S. 252.

VI. Anordnung der Auskunftserteilung und Begründung

Die Anordnung der Auskunftserteilung über Verkehrsdaten bedarf gemäß § 100h I Satz 3 i. V. m. § 100b I Satz 1 StPO in der Regel eines gerichtlichen Beschlusses. Nur bei Gefahr im Verzug darf die Verkehrsdatenabfrage gemäß § 100h I Satz 3 i. V. m. § 100b I Satz 2 StPO durch die Staatsanwaltschaft angeordnet werden. Eine Eilbefugnis für Ermittlungspersonen der Staatsanwaltschaft wurde nicht eingeführt.[197]

Gefahr im Verzug liegt dann vor, wenn die vorherige Einholung der richterlichen Anordnung den Erfolg der Maßnahme gefährden würde.[198] Gemäß § 100g I Satz 3 StPO i. V. m. § 100b I Satz 3 StPO tritt die Anordnung der Staatsanwaltschaft außer Kraft, wenn nicht innerhalb von drei Tagen eine richterliche Bestätigung erfolgt. Umstritten ist, ob es für die Wirksamkeit der Eilanordnung für diese drei Tage immer einer richterlichen Bestätigung bedarf oder nur dann, wenn über den Zeitraum von drei Tagen hinaus weitere Daten benötigt werden.

In der Literatur wird überwiegend vertreten, dass Eilanordnungen der Staatsanwaltschaft auch im Falle fehlender richterlicher Bestätigung nicht nachträglich unwirksam werden.[199] Die Verpflichteten seien gehalten, auf eine entsprechende Eilanordnung Auskünfte zu erteilen, auch wenn eine anschließende richterliche Bestätigung nicht erfolge und die Drei-Tages-Frist bereits vor der Auskunftserteilung abgelaufen sei.[200] Die bis zu diesem Zeitpunkt erlangten Erkenntnisse bleiben demnach grundsätzlich verwertbar.[201] Die Regelung hat nach dieser Auffassung nur Bedeutung für zukünftige und über einen Zeitraum von mehr als drei Tagen hinaus reichende Verbindungsabfragen.[202] Begründet wird der Verzicht auf eine richterliche Bestätigung damit, dass die Auskunftserteilung unverzüglich zu erfolgen habe und die Maßnahme daher innerhalb der drei-Tages-Frist erledigt sei.[203] Herangezogen wird im Übrigen ein Umkehrschluss aus § 98b I Satz 2, § 100d I Satz 2 und § 163d I Satz 2 StPO.[204] Die Rechtmäßigkeit der durchgeführten Maßnahme sei auch nicht Gegenstand der richterlichen Bestätigung, sondern nur die Entscheidung darüber, ob die Voraussetzungen zum Zeitpunkt des richterlichen Beschlusses noch vorliegen und die Maßnahme dementsprechend fortdauern soll.[205]

Fraglich ist dann aber, welche Funktion die richterliche Bestätigung in diesem Fall noch hat und ob der Verzicht auf die richterliche Bestätigung aus dem Blickwinkel des Rechtsstaatsprinzips vertretbar ist. Liegt kein Eilfall vor und ist der Richter zu erreichen, dann muss eine umfassende Rechtmäßigkeitsprüfung stattfinden. Der oberflächliche Grund für den Verzicht auf eine richterliche Bestätigung liegt demnach in der Unerreichbarkeit des Richters. Hierin liegt das Risiko einer Aushebelung des Richtervorbehalts. Der Verzicht auf die Bestätigung lässt sich nur schwer mit dem Anspruch auf effektiven Rechtsschutz vereinbaren. Dem Grundsatz eines wirksamen Rechtsschutzes entspricht zunächst die präventive richterliche Kontrolle. Kann diese wegen Eilerwägungen nicht stattfinden, dann tritt an ihre Stelle (und als notwendiger Ausgleich) die post facto durchgeführte richterliche Prüfung.[206] Auch der Vergleich mit Eilkompetenzregelungen zu anderen Ermittlungsmaßnahmen spricht für diese Auslegung. Wenn beispielsweise eine Beschlagnahme oder eine Rasterfahndung von der Staatsanwaltschaft angeordnet wurde, so muss diese (bei der Beschlagnahme nur bei Vorliegen weiterer Voraussetzungen) binnen drei Tagen gemäß § 98 II Satz 1 StPO bzw. 98b I Satz 2 StPO richterlich bestätigt werden. Wenn diese Maßnahmen aber innerhalb dieser Zeit durchgeführt wurden, wovon aufgrund des Eilfalls auszugehen ist, macht es keinen Sinn, eine richterliche Bestätigung für eine *Fortdauer* der Maßnahmen einzuholen. Die Maßnahmen sind bereits abgeschlossen. Ein entsprechendes Modell dürfte auch für die Verkehrsdatenabfrage in Betracht zu ziehen sein.

Zudem ist die Anordnungskompetenz des Richters das nötige Korrektiv zur Heimlichkeit und Eingriffstiefe der Maßnahme.[207] Der Richtervorbehalt zielt auf eine vorbeugende Kontrolle der Maßnahme durch eine unabhängige und neutrale Instanz. Erst die Einschaltung des Richters gewährleistet den geforderten effektiven Rechtsschutz.[208] Wenn dem Richtervorbehalt aber eine solche Funktion zugewiesen wird, dann ist nicht nachzuvollziehen, warum dem Betroffenen dieser Schutz nur deshalb nicht zuteil kommen soll, weil der Richter vor Anordnung der Verkehrsdatenabgabe nicht erreichbar war.

Problematisch gestaltete sich früher auch die Zuständigkeit des Gerichts. Unklar war, ob das Gericht am Sitz des Telekommunikationsunternehmens für die Anordnung der Verkehrsdatenabfrage zuständig ist oder das Gericht am Sitz einer Zweigstelle, in der die Daten erhoben werden. Der *Bundesgerichtshof* klärte diese Frage im Jahre 2003 mit der Entscheidung, aus § 162 I Satz 1 StPO folge die Zuständigkeit des Gerichts, in dessen Bezirk die Verkehrsdaten zu erheben und die Auskünfte zu erteilen sind.[209]

Anforderungen an die Begründung der Anordnung durch den Richter und im Eilfall durch den Staatsanwalt sind im Gesetz nicht konkretisiert worden. Festgelegt ist nur, dass

---

[197] *Nack*, in: Karlsruher Kommentar, 2003, § 100b Rn. 1.
[198] BVerfGE 51, S. 97, 111.
[199] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100h Rn. 4; vgl. auch *Günther,* in: BKA (Hrsg.), 2004, S. 60.
[200] *Bock*, in: Beck'scher TKG-Kommentar, 2006, § 110 Rn. 69.
[201] *Bär*, MMR 2002, S. 363.
[202] *Bär*, MMR 2002, S. 363; *Günther,* in: BKA (Hrsg.), 2004, S. 60; *Nack*, in: Karlsruher Kommentar, 2003, § 100h Rn. 1.
[203] *Bär*, MMR 2002, S. 363.
[204] *Nack*, in: Karlsruher Kommentar, 2003, § 100h Rn. 1.
[205] *Bock*, in: Beck'scher TKG-Kommentar, 2006, § 110 Rn. 69; *Günther,* in: BKA (Hrsg.), 2004, S. 60.
[206] *Schäfer,* in: Löwe-Rosenberg, 2004, § 100b Rn. 23.
[207] *Schäfer,* in: Löwe-Rosenberg, 2004, § 100a Rn. 110; *Wohlers*, in: SK StPO, 2006, § 162 Rn. 4.
[208] BVerfGE 103, S. 142, 151; BVerfG NJW 2001, S. 1121, 1122; BVerfG NStZ 2003, S. 441, 442.
[209] BGH 2 ARs 252/02 v. 6. September 2002, NStZ 2003, S. 163; BGH 2 ARs 276/02 v. 13. September 2002, NStZ-RR 2002, S. 369; BGH (mit Anmerkung *Bär*), MMR 2003, S. 266.

die Anordnung schriftlich ergehen muss und Art, Umfang und Dauer der Maßnahmen hinreichend zu bestimmen sind (§§ 100h I Satz 3, 100b II Satz 1, 3 StPO). Insoweit ist es Aufgabe des erlassenden Organs, den Eingriff in die grundrechtlich geschützte Sphäre des Bürgers angemessen zu begrenzen[210]. Dem Richter ist eine genaue Festlegung aufgegeben, ob abgehende oder ankommende Anrufe abgefragt werden sollen und welche Standorte oder Funkzellen erfasst sind. Der Zeitraum, für den Daten abgefragt werden sollen, muss konkretisiert werden und insbesondere bei der Funkzellenabfrage ist der räumliche Bereich (und damit der Umfang) zu begrenzen. Wie die Untersuchung von *Albrecht/Dorsch/Krüpe* gezeigt hat, bestehen – zumindest bei der Anordnung von Telekommunikationsüberwachungsmaßnahmen – erhebliche Defizite bei der Begründung durch den Richter. Nur 23,5 Prozent der überprüften Beschlüsse wurden in der Untersuchung als substantiell begründet bewertet.[211] Zu ähnlichen Ergebnissen kam auch die Studie von *Backes/ Gusy*[212]. Diese bezeichneten es sogar als wahrscheinlich, dass die Richter die staatsanwaltschaftlichen Ausführungen inhaltlich oder sogar wörtlich unkritisch übernehmen und ihrer gesetzlich vorgeschriebenen Kontrollfunktion nur unzureichend nachkommen.

Die Anordnung muss nach § 100h I Satz 1 StPO den Namen und die Anschrift des Betroffenen, gegen den sie sich richtet, sowie die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten. Im Falle einer Straftat von erheblicher Bedeutung genügt gemäß § 100h I Satz 2 StPO eine *räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation,* über die Auskunft erteilt werden soll, wenn andernfalls die Erforschung des Sachverhalts aussichtslos oder wesentlich erschwert wäre. Letztere Regelung betrifft (vor allem) die Funkzellenabfrage.

Die Regelung des § 100 h Satz 2 StPO ist vielfacher Kritik ausgesetzt. Reichweite und Bedeutung der Pflicht zur Bezeichnung des Betroffenen sind demnach nicht klar genug bestimmt.[213] Weit verbreitet ist die Ansicht, dass aufgrund der gewählten Formulierung Ermittlungshindernisse bei Straftaten mit unbekanntem Täter auftreten können. Insbesondere wird geltend gemacht, dass die Aufklärung von Straftaten, die über das Internet begangen werden, erschwert sei.[214] Denn der Inhaber einer IP-Adresse oder der für eine Homepage Verantwortliche seien häufig namentlich nicht bekannt. Auch bei Internet-Bestellungen unter falschem Namen steht regelmäßig nur die verwendete IP-Adresse fest.[215] Bei beleidigenden oder bedrohenden Anrufen ist zunächst nur die Nummer des anrufenden Anschlusses bekannt.[216] Ein Teil der Literatur forderte deshalb, dass die Anordnung gegen einen namentlich nicht bekannten, aber individualisierbaren Betroffenen immer zulässig sein müsse.[217] Nach dem Wortlaut des § 100h I Satz 1 StPO ist dies jedoch nach teilweise vertretener Ansicht nicht möglich.[218] Zum Teil wird auch angenommen, dass die in § 100h I Satz 1 StPO geforderten Angaben nur aufgeführt werden müssen, wenn der Täter bekannt ist, dagegen nicht bei Ermittlungen gegen unbekannt.[219]

Die Anordnung setzt eine richterliche Einzelfallprüfung voraus, die sich auf die Eingriffsvoraussetzungen und die Angemessenheit des Eingriffs im konkreten Einzelfall bezieht.[220] Sie enthält auch die dem Beschuldigten zur Last gelegte Straftat sowie den Grund der Überwachung unter Angabe der Verdachts- und Beweislage, die die Maßnahme rechtfertigt.[221] Der Bundesgerichtshof fordert die Darlegung der den Tatverdacht begründenden Tatsachen und der Beweislage auch für die Begründung einer richterlichen Bestätigung.[222] Allerdings genügt dabei im Einzelfall auch eine konkrete Bezugnahme auf Aktenteile. Ob die Verhältnismäßigkeitsprüfung, insbesondere auch die Auseinandersetzung mit dem Subsidiaritätsgrundsatz, ebenfalls schriftlich erfolgen muss, ist nicht ausdrücklich festgelegt. Das Bundesverfassungsgericht hat jedenfalls ausgeführt, dass es Aufgabe und Pflicht des Ermittlungsrichters sei, sich eigenverantwortlich ein Urteil zu bilden und nicht die Anträge der Staatsanwaltschaft nach einer nur pauschalen Überprüfung gegenzuzeichnen.[223] Die Eingriffsvoraussetzungen müssten sorgfältig geprüft werden und eine umfassende Abwägung zur Feststellung der Angemessenheit des Eingriffs im konkreten Fall erfolgen. Dies entspricht dem Anspruch an eine die „gründliche und umfassende Überprüfung“ der Voraussetzungen[224] nachvollziehende Begründung[225], mit der Selbstkontrolle[226] und die Überprüfung im Rechtsmittelverfahren[227] erst ermöglicht werden[228].

Umstritten ist schließlich, ob eine Anordnung bei Vorliegen einer Einwilligungserklärung des Betroffenen entbehrlich ist. Teilweise wird vertreten, dass der Betroffene dadurch auf den Schutz seines Fernmeldegeheimnisses zulässigerweise verzicht[229]. Die Kommunikationsbeteiligten hätten das Recht zu entscheiden, ob sie Kommunikation geschlossen halten oder anderen zugänglich ma-

---

[210] *Wohlers/Demko*, StV 2003, S. 244.
[211] *Albrecht/Dorsch/Krüpe*, 2003, S. 447.
[212] *Backes/Gusy*, 2003, S. 48 ff.
[213] *Wolff/Neumann*, NStZ 2003, S. 404.
[214] *Nack*, in: Karlsruher Kommentar, 2003, § 100h Rn. 5.
[215] *Wolff/Neumann*, NStZ 2003, S. 404.
[216] *Wolff/Neumann*, NStZ 2003, S. 404.
[217] *Meyer-Goßner*, 2006, § 100h Rn. 3.
[218] *Wolff/Neumann*, NStZ 2003, S. 404.
[219] LG Ulm, Beschluss v. 21.3.2002 § 2 Qs 2016/02; LG Dortmund mit Anmerkung *Bär*, MMR 2003, S. 54, 55; AG Köln mit Anmerkung *Bär*, MMR 2003, S. 611, 612; *Bär*, MMR 2002, S. 363.
[220] BVerfG NStZ 2003, S. 441; *Gusy*, NStZ 2003, S. 403; *Meyer-Goßner*, 2006, § 100h Rn. 3.
[221] BGHSt 47, S. 362; *Kinzig*, StV 2004, S. 562; *Meyer-Goßner*, 2006, § 100a Rn. 3; *Pfeiffer*, 2005, § 100b Rn. 2.
[222] BGHSt 47, S. 362; so auch *Pfeiffer*, 2005, § 100b Rn. 2.
[223] BVerfG NJW 2003, S. 1787, 1792; BVerfG NStZ 2003, S. 441, 443.
[224] BGH NStZ 1995, S. 510, 511.
[225] *Backes/Gusy*, StV 2003, S. 249; *Schäfer*, in: *Löwe-Rosenberg,* 2004, § 100h Rn. 16.
[226] BGHSt 47, S. 362, 366.
[227] BGHSt 47, S. 362, 366; *Schäfer*, in: *Löwe-Rosenberg,* 2004, § 100h Rn. 16.
[228] BVerfGE 42, S. 212, 220; *Wohlers*, in: SK StPO, 2006, § 162 Rn. 30.
[229] BGH NJW 1994, S. 596, 597; *Dreier*, in: *Dreier,* 2004, Vorbem. Rn. 129; *Dürig*, in: *Maunz/Dürig,* 2006, Artikel 10 GG Rn. 30.

chen wollen.[230] Das gelte auch dann, wenn der Dritte ohne Wissen und Wollen des anderen Kommunikationspartners beteiligt wird.[231] Ganz überwiegend wird es jedoch als nicht ausreichend angesehen, wenn nur ein Beteiligter des Telekommunikationsvorgangs die Einwilligung erklärt[232], da die Einwilligung eines Teilnehmers an der Telekommunikation nicht mit Wirkung für einen anderen Teilnehmer ausgestattet sei.[233] Erforderlich ist demnach die Zustimmung aller Kommunikationsteilnehmer.[234]

VII. Dauer der Maßnahme

Wie bei der Überwachung des Inhalts der Telekommunikation ist auch bei der Verkehrsdatenabfrage der Zeitraum der zulässigen Überwachung *zukünftiger* Telekommunikationsverbindungen beschränkt (§ 100h I Satz 3 StPO). Die Anordnung kann für höchstens drei Monate erfolgen (§ 100h I Satz 3 i. V. m. § 100b II Satz 4 StPO). Eine zeitliche Begrenzung für eine Abfrage von Daten, die bereits entstanden sind, ist im Gesetz nicht enthalten. Daten, die noch verfügbar sind, können abgefragt werden. Der Abfragezeitraum wird demnach durch die jeweilige Praxis der Speicherungsdauer einzelner Netzbetreiber und die Regeln des TKG begrenzt. Bei Wegfall der Anordnungsvoraussetzungen für die in die Zukunft gerichtete Verkehrsdatenabfrage ist die Maßnahme gemäß § 100h I Satz 3 i. V. m. § 100b IV StPO unverzüglich zu beenden. Bei der Abfrage von Verkehrsdaten, die in die Zukunft gerichtet ist, ist ferner eine Verlängerungsmöglichkeit für die Dauer von jeweils höchstens drei Monaten vorgesehen (§ 100h I Satz 3 i. V. m. § 100b II Satz 5 StPO).

VIII. Durchführung der Maßnahme

Die Durchführung der Maßnahme obliegt der Staatsanwaltschaft. Sie hat dem Betreiber der Fernmeldeanlagen die Anordnung mitzuteilen.[235] Auskunftspflichtig sind diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken (§ 100g I Satz 1 StPO), also Anbieter i. S. v. § 3 Nr. 6 TKG. Danach ist Telekommunikationsdiensteanbieter jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Zu den Diensteanbietern gehören Festnetz- und Mobilfunknetzbetreiber, Servicebetreiber sowie Internet-Service-Provider, soweit sie Telekommunikationsdienste wie Internettelefonie anbieten.[236] Dabei haben sie die Auskunft unverzüglich zu erteilen, d. h. ohne schuldhaftes Zögern.[237] Überschreitet der Anbieter die Art und den Umfang der Auskunft, wie sie in einer Anordnung festgelegt ist, so erfüllt dies den Tatbestand des § 206 I StGB.[238]

Umstritten ist, inwiefern die Telekommunikationsunternehmen dabei eine Prüfungspflicht bzw. ein Prüfungsrecht bzgl. der Anordnungen haben. Gemäß § 88 II TKG sind die Diensteanbieter nämlich zur Wahrung des Fernmeldegeheimnisses verpflichtet. Die Anbieter befinden sich also in der Konfliktlage, einerseits § 88 TKG beachten und andererseits der Verpflichtung aus § 100g StPO gerecht werden zu müssen. Nach herrschender Meinung haben die Anbieter jedoch nicht die rechtlichen bzw. sachlichen Voraussetzungen für die angeordnete Maßnahme zu überprüfen.[239] Mit der Annahme eines materiellen Prüfungsrechts wäre freilich eine zu starke Behinderung der Ermittlungsbehörden verbunden.[240] Telekommunikationsunternehmen sind im Übrigen „weder private Ermittlungsorgane noch besteht Anlass, ihnen die Hintergründe der Anordnung zu offenbaren“[241]. Insoweit fehlt bereits eine ausreichende Informationsgrundlage.[242] Dagegen müssen die Anbieter die formellen Voraussetzungen einer Anordnung nach §§ 100g, 100h StPO überprüfen [243], bei Fehlerhaftigkeit die Auskunft verweigern und damit unberechtigte staatliche Eingriffe in das Fernmeldegeheimnis verhindern.[244]

Bei Auskunftsverweigerung können Ordnungs- oder Zwangsmittel verhängt werden (§ 100h I Satz 3 i. V. m. § 95 II i. V. m. § 70 StPO). Wegen der Verpflichtung zur *unverzüglichen* Auskunftserteilung kommt bei einer signifikanten Verzögerung der Ermittlungshandlungen eine Strafbarkeit wegen Strafvereitelung in Betracht.[245] Den Verpflichteten steht gegen richterliche Beschlüsse die Beschwerde nach § 304 StPO zur Verfügung.[246]

Die Art und Weise der Durchführung ist im Einzelnen im Gesetz nicht geregelt. Zweckmäßig erscheint es, zur Erleichterung der Weiterverarbeitung die Daten auf elektronischen Speichermedien und nicht in Papierform zu übermitteln[247]. Nach einem Bundesgerichtshof-Ermittlungsrichterbeschluss vom 20. März 2003[248] können der Ermittlungsrichter und im Grundsatz auch die Staatsanwaltschaft die Modalitäten der Übermittlung unter Berücksichtigung der Verhältnismäßigkeit bestimmen. Die gesetzlichen Vorschriften zur Verkehrsdatenabfrage enthalten danach konkludent die Ermächtigung zur Anordnung solcher Begleitmaßnahmen, die mit der Übermitt-

---

[230] BGH NJW 1994, S. 596, 597.
[231] BGH NJW 1994, S. 596, 597.
[232] BVerfGE 85, S. 386, 398; *Bock,* in: Beck'scher TKG-Kommentar, 2006, § 88 Rn. 56; *Hermes*, in: *Dreier,* 2004, Artikel 10 Rn. 55; *Krüger*, in: Sachs, 1999, Artikel 10 GG Rn. 43.
[233] BVerfGE 85, S. 386, 399.
[234] *Hermes*, in: *Dreier,* 2004, Artikel 10 Rn. 55.
[235] *Pfeiffer*, 2005, § 100b Rn. 3.
[236] *Bock*, in: Beck'scher TKG-Kommentar, 2006, § 88 Rn. 22.
[237] *Bock*, in: Beck'scher TKG-Kommentar, 2006, § 88 Rn. 22; § 121 I BGB.
[238] *Gnirck/Lichtenberg*, DuD 2004, S. 602; *Sankol*, JuS 2006, S. 703.
[239] Ermittlungsrichter des BGH, CR 1998, S. 738, 739; *Friedrich*, 2001, S. 80; *Gnirck/Lichtenberg*, DuD 2004, S. 602; *Günther*, in: BKA (Hrsg.), 2004, S. 66; *Meyer-Goßner*, 2006, § 100g Rn. 8; *Sankol*, JuS 2006, S. 701; *Wolff/Neumann*, NStZ 2003, S. 407.
[240] Ermittlungsrichter des BGH, CR 1998, S. 738, 739.
[241] *Wolff/Neumann*, NStZ 2003, S. 407.
[242] *Friedrich*, 2001, S. 80.
[243] OLG Hamm DuD 2000, S. 234; *Friedrich*, 2001, S. 80.
[244] *Wolff/Neumann*, NStZ 2003, S. 407; OLG Hamm, DuD 2000, S. 234.
[245] BGHR StGB § 258 I Vollendung 1; *Nack*, in: Karlsruher Kommentar, 2003, § 100g Rn. 3.
[246] *Meyer-Goßner*, 2006, § 100b Rn. 10.
[247] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 31.
[248] BGH 1 BGs 107/2003, Beschluss vom 20. März 2003; Ermittlungsrichter des BGH, NStZ 2005, S. 278.

lung der Daten notwendig verbunden sind. Da die Auswertung einer großen Datenmenge auf Papier zu hohem Zeitaufwand und einer größeren Fehlerquote führt, die Netzbetreiber im Übrigen ohne zusätzliche Belastung elektronisch gespeicherte Daten zur Verfügung stellen können, ist die Verpflichtung zur Übermittlung elektronischer Daten gerechtfertigt.

Schließlich wird darauf verwiesen, dass sich Lücken, Unklarheiten und Widersprüche der gesetzlichen Vorschriften negativ auf die Zusammenarbeit zwischen Strafverfolgungsbehörden und Diensteanbietern auswirken.[249] Erhebliche Rechtsunsicherheit wird hinsichtlich der gesetzlichen Voraussetzungen für Auskunftsverlangen im Bereich der Internet-Nutzung festgestellt.[250] In der Rechtsunsicherheit wird ein Grund für Verweigerungen der Mitwirkung im Einzelfall gesehen.[251] Deshalb wird die Herstellung von Normenklarheit angemahnt, mit dem Ziel, eine konfliktfreie und reibungslose Zusammenarbeit zwischen den Strafverfolgungsbehörden und den Service-Providern zu sichern.[252]

Die durch die Auskunft erlangten Unterlagen sind unverzüglich zu vernichten, wenn sie zur Strafverfolgung nicht mehr erforderlich sind (§§ 100h I Satz 3 i. V. m. 100b VI StPO). Die Vernichtungsregelung des § 100b VI StPO gilt entsprechend.[253] Die Staatsanwaltschaft hat darüber Aufsicht zu führen und eine Niederschrift anzufertigen.

IX. Betroffene und Benachrichtigung

Auskunft erteilt werden darf nur über Verkehrsdaten des Beschuldigten und der sog. Nachrichtenmittler.[254] Dies sind Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt (§§ 100g I Satz 2 i. V. m. 100a Satz 2 StPO). Dabei spielt es keine Rolle, ob diese Personen von der Nutzung ihres Anschlusses durch den Beschuldigten oder davon wissen, dass sie Mitteilungen entgegennehmen. Es kommt dabei auch nicht auf den Willen an, Nachrichten vom Beschuldigten entgegenzunehmen. Gutgläubigkeit steht der Anordnung nicht entgegen.[255] Bei Hacker-Angriffen unter Ausnutzung von Computernetzwerken sind die Betreiber von dazu missbrauchten, zwischengeschalteten Computernetzwerken Nachrichtenmittler.[256] Auch das Opfer einer Straftat (z. B. einer Erpressung oder Beleidigung) nimmt Mitteilungen vom Beschuldigten entgegen.[257]

Anlässlich der Verkehrsdatenabfrage sind unbeteiligte Dritte notwendigerweise betroffen.[258] Die Überwachung wird deshalb aber nicht unzulässig.[259] Gemäß § 101 I StPO sind die von der Verkehrsdatenabfrage Betroffenen (Beteiligten) allerdings zu benachrichtigen. Dies gilt nicht nur für Maßnahmen nach §§ 100g, 100h StPO, sondern auch für solche nach §§ 81e, 99, 100a, 100b sowie 100f I Nr. 2, II StPO. Den Beteiligten wird nachträglich rechtliches Gehör gewährt,[260] das im Vorfeld der Maßnahme wegen der Gefährdung des Untersuchungszwecks nicht möglich war. Beteiligte sind alle von den Maßnahmen unmittelbar Betroffenen.[261] Auch Zielpersonen und ihre Gesprächspartner können Beteiligte sein, jedoch nicht zufällig (unvermeidbar) betroffene unbeteiligte Dritte.[262] So sind beispielsweise bei einer Zielwahlsuche oder Funkzellenabfrage diejenigen Anrufer, deren Anruf keine Beweisbedeutung hat, nicht zu benachrichtigen.[263] In diesen Fällen sind den Ermittlern lediglich die Rufnummern und nicht die Anschlussinhaber bekannt. Die Zuordnung der Rufnummern zu einer bestimmten Person, die für eine Benachrichtigung notwendig wäre, würde daher den Grundrechtseingriff nur verstärken. Der Sinn der Benachrichtigungspflicht besteht aber in einer Begrenzung des Grundrechtseingriffs und nicht in deren Verstärkung.

Eine Benachrichtigung darf jedoch nur stattfinden, wenn dies ohne Gefährdung des Untersuchungszwecks, der öffentlichen Sicherheit, von Leib oder Leben einer Person sowie der Möglichkeit der weiteren Verwendung eines eingesetzten, nicht offen ermittelnden Beamten geschehen kann (§ 101 I Satz 1 StPO). Wenn die Verkehrsdaten also im laufenden Verfahren oder auch in anderen Verfahren gegen den Beschuldigten oder Mitbeschuldigte weiterhin benötigt werden und der Ermittlungserfolg durch die Benachrichtigung beeinträchtigt werden könnte, wird die Benachrichtigung zunächst zurückgestellt. Das Bundesverfassungsgericht hat in der Entscheidung zur akustischen Wohnraumüberwachung die Zurückstellung der Benachrichtigung eingeengt[264]. Für die Ausführung der Benachrichtigung ist die Staatsanwaltschaft zuständig.[265] Die Telekommunikationsunternehmen sind den Beteiligten gegenüber zum Schweigen verpflichtet.[266]

Auch in Bezug auf die Benachrichtigungspflicht zeigten die Untersuchungen zu §§ 100a, 100b StPO für Zeiträume vor 2000 Defizite auf. Im Rahmen der Untersuchung des MPI zur Telekommunikationsüberwachung wurde festgestellt, dass nur in 15,3 Prozent der Fälle in den Akten ausdrücklich niedergelegt wurde, dass eine Benachrichtigung

[249] *Günther,* in: BKA (Hrsg.), 2004, S. 57.
[250] *Königshofen,* in: BKA (Hrsg.), 2004, S. 78.
[251] *Günther,* in: BKA (Hrsg.), 2004, S. 57.
[252] *Günther,* in: BKA (Hrsg.), 2004, S. 57; *Königshofen,* in: BKA (Hrsg.), 2004, S. 79.
[253] *Schäfer*, in: Löwe-Rosenberg, 2004, § 100h Rn. 33.
[254] *Meyer-Goßner*, 2006, § 100a Rn 11.
[255] *Beulke*, Jura 1986, S. 643; *Meyer-Goßner*, 2006, § 100a Rn. 11; vgl. auch *Sankol*, JuS 2006, S. 700.
[256] Bundestagsdrucksache 14/7008, S. 7; *Bär*, MMR 2002, S. 362; *Meyer-Goßner*, 2006, § 100g Rn. 9; *Nack*, in: Karlsruher Kommentar, 2003, § 100g Rn. 5; *Beulke*, Jura 1986, S. 643; *Meyer-Goßner*, 2006, § 100a Rn. 12; *Pfeiffer*, 2005, § 100a Rn. 7.
[257] *Nack*, in: Karlsruher Kommentar, 2003, § 100a Rn. 25; *Schmidt*, Der Kriminalist 2002, S. 213.
[258] BVerfGE 30, S. 1, 22.
[259] BVerfGE 30, S. 1, 22.
[260] *Nack,* in: Karlsruher Kommentar, 2003, § 101 Rn. 1; *Pfeiffer*, 2005, § 101 Rn. 1.
[261] *Pfeiffer*, 2005, § 101 Rn. 1.
[262] *Pfeiffer*, 2005, § 101 Rn. 1.
[263] *Nack,* in: Karlsruher Kommentar, 2003, § 101 Rn. 3.
[264] BVerfG, 1 BvR 2378/98 vom 3. März 2004, Absatz-Nr. 288ff.
[265] BGHSt 36, S. 305, 311.
[266] *Meyer-Goßner*, 2006, § 101 Rn. 8.

des Anschlussinhabers stattfand.[267] In 12 Prozent der Fälle wurde eine anderweitige Kenntniserlangung insbesondere durch Akteneinsicht angenommen. Entsprechendes ergibt sich aus der Bielefelder Untersuchung. Dort wurden nur in 2,3 Prozent der Fälle die Betroffenen ausdrücklich benachrichtigt, während bei 50 Prozent davon ausgegangen werden kann, dass der Beschuldigte durch die Akteneinsicht eines Rechtsanwalts von der Maßnahme Kenntnis erlangt hat.[268]

X. Zeugnisverweigerungsberechtigte

§ 100h II Satz 1 StPO verbietet Auskunftsverlangen über Telekommunikationsverbindungen, die von oder zu einem Zeugnisverweigerungsberechtigten nach § 53 I Satz 1 Nr. 1, 2 und 4 StPO hergestellt werden. Soweit Geistlichen, Verteidigern oder Mitgliedern des Bundes- oder eines Landtages ein Zeugnisverweigerungsrecht zusteht, dürfen Verkehrsdaten nur dann abgefragt werden, wenn diese selbst unter dem Verdacht der Teilnahme, Begünstigung, Strafvereitelung oder Hehlerei stehen (§ 100h II Satz 2 StPO). Wenn Daten gleichwohl erhoben wurden (weil das Zeugnisverweigerungsrecht bei Datenerhebung nicht ersichtlich war), besteht ein Verwertungsverbot (§ 100h II Satz 1, 1.HS. StPO).

Für die Begrenzung des Verwertungsverbots in Bezug auf Daten, die von Zeugnisverweigerungsrechten dieses speziellen Personenkreises betroffen sind, wird in der Gesetzesbegründung[269] angeführt, dass die Einbeziehung Geistlicher dem Vertrauen in die absolute Privatheit einer Kontaktaufnahme zu einem geistlichen Seelsorger Rechnung trage. Die Berücksichtigung von Verteidigern und Parlamentariern wird mit deren für die demokratische Verfassung bedeutsamen „staatskonstituierenden Kontrollfunktion“ begründet. Unklar bleibt aber, warum diese Berufsgruppen in § 100h StPO besonders berücksichtigt werden, in vergleichbaren Vorschriften dagegen nicht. So fehlt die Regelung eines Verwertungsverbots in §§ 100a, 100b StPO gänzlich, obwohl auch diese Vorschriften das Fernmeldegeheimnis tangieren und die Telekommunikationsüberwachung durch die Preisgabe des Inhalts der Telekommunikation einen intensiveren Eingriff darstellt. Dagegen geht das Beweisverwertungsverbot in § 100c VI StPO weiter als das des § 100h II StPO, da hier alle Fälle des §§ 52, 53 StPO und die Berufshelfer (§ 53a StPO) erfasst werden.

Die Vereinheitlichung der Regelungen zu Zeugnisverweigerungsberechtigten wird deshalb als dringend geboten angesehen.[270] Zwar können Zeugnisverweigerungsrechte im Rahmen der Verhältnismäßigkeitsprüfung besondere Berücksichtigung finden (dies ist auch vom Bundesverfassungsgericht für Mitarbeiter der Medien ausdrücklich hervorgehoben worden[271]), doch sollte nach fast einhelliger Auffassung eine konsistente und transparente Regelung für alle verdeckten Ermittlungsmaßnahmen an die Stelle der jetzigen Lösung treten,[272] die als „uneinheitlich, unvollkommen und unausgewogen“[273] bezeichnet wird.

Freilich geht es nicht nur um die formale Vereinheitlichung der Behandlung der Zeugnisverweigerungsrechte im Rahmen verdeckter Ermittlungsmaßnahmen. Es geht insbesondere um die Frage wie weit der Schutz verschiedener Berufsgruppen reichen soll und ob auch Berufshelfer einbezogen werden sollen[274]. In neuerer Zeit ist die Berufsgruppe der Journalisten in das Zentrum der Debatten gerückt[275]. Das Interesse von Strafverfolgungsbehörden und Geheimdiensten an Journalisten ist ebenso einfach begründet wie das Interesse von Journalisten an Strafverfolgungsbehörden, Geheimdiensten sowie deren Klientel. Journalisten sind an sicherheitsrelevanten Informationen interessiert und vermögen sich diese auch zuweilen zu beschaffen. Sicherheitsrelevante Informationen beziehen sich auf Praktiken der Strafverfolgungsbehörden und der Geheimdienste sowie auf Praktiken derer, von denen Sicherheitsprobleme ausgehen, also Terroristen, Mafiosi, Großbetrüger etc. Hieraus ergeben sich Konflikte, die der Presse- und Rundfunkfreiheit einerseits sowie dem Interesse an Strafverfolgung, an einer funktionsfähigen Strafrechtspflege, an der Ermittlung der Wahrheit und an Sicherheit im Allgemeinen geschuldet sind. Die Spannungen zwischen Pressefreiheit, Strafverfolgung und Sicherheit setzen sich auf den europäischen und internationalen Ebenen fort. Die Empfehlungen des Europarats aus dem Jahre 2000 zum Schutz der Presse im Zusammenhang mit Maßnahmen der Strafverfolgung und vor dem Hintergrund der Europäischen Menschenrechtskonvention legen hierüber Zeugnis ab[276]. Das Gewicht des Schutzes der Pressefreiheit wird in Artikel 5 Grundgesetz und in den europäischen und internationalen Bürgerrechtskonventionen sichtbar. Die Bedeutung einer freien Berichterstattung (die den Zugang zu sensiblen politischen Informationen selbstverständlich einschließt) ist dabei unumstritten. Sie zeigt sich nicht nur in ihrer Relevanz für die Gewährleistung der Menschenrechte selbst sowie der demokratischen Verfassung von Gesellschaften, sondern auch in der Relevanz für die Prävention von Korruption und anderen Formen der organisierten Kriminalität. Freilich sind Pressefreiheit und der Schutz von Journalisten nicht abwägungsfest. Die Pressefreiheit tritt zunehmend in ein Konkurrenzverhältnis nicht nur zu Interessen an Strafverfolgung, sondern zum Interesse an der Herstellung von Sicherheit.

Die Reformen der Strafprozessordnung der letzten Jahre verweisen jedenfalls auf eine Gemengelage des Interesses der Politik an der Berücksichtigung von Medienschutz und an einer effizienten Gewährleistung von Sicherheit vor Terrorismus und transnationaler organisierter Krimi-

[267] *Albrecht/Dorsch/Krüpe*, 2003, S. 276.
[268] *Backes/Gusy*, StV 2003, S. 251.
[269] Bundestagsdrucksache 14/7679, S. 9.
[270] *Keller*, Die Polizei 2005, S. 112; *Meyer-Goßner*, 2006, § 100h Rn. 9.
[271] BVerfG NJW 2003, S. 1787, 1794; *Schäfer*, in: Löwe-Rosenberg, 2004, § 100h Rn. 28.
[272] *Wohlers/Demko*, StV 2003, S. 246.
[273] *Wolter/Schenke*, 2002, S. 33.
[274] *Wolter/Schenke*, 2002, S. 35; *Wolter*, in: SK StPO, 2006, § 100h Rn. 6; *Welp*, GA 2002, S. 550; *Wohlers/Demko*, StV 2003, S. 246.
[275] *Wolter/Schenke*, 2002, S. 35; *Welp*, GA 2002, S. 550; *Wohlers/Demko*, StV 2003, S. 246; *Wollweber*, NJW 2002, S. 1554, 1555 unter Verweis auf BVerfGE 91, S. 125, 134.
[276] Recommendation No. R (2000) 7 on the right of journalists not to disclose their sources of information.

nalität. Im Jahre 2002 trat eine Änderung der Strafprozessordnung in Kraft, die in § 53 I Nr. 5 StPO den Schutz der Pressefreiheit in Form einer Erweiterung des Zeugnisverweigerungsrechts für Journalisten deutlich – und wie gesagt wird: verfassungsrechtlich nicht zwingend[277] – verstärkte. Die Beschlagnahmeregelungen sehen in § 97 V StPO einen besonderen Schutz für Journalisten vor. Zur gleichen Zeit trat allerdings eine Änderung der Strafprozessordnung in Kraft, die in Gestalt der §§ 100g, 100h StPO eine weitgehende Nutzung von TelekommunikationsVerkehrsdaten ermöglicht und dabei zwar die Zeugnisverweigerungsrechte des § 53 I StPO für Rechtsanwälte, Seelsorger und Parlamentarier in §100 h II StPO honoriert, Journalisten aber ausnimmt. Der Begründung des Gesetzes lässt sich für die Beschränkung kaum etwas entnehmen; freilich erstreckt die Neuregelung der akustischen Wohnraumüberwachung in § 100c VI Satz 1 StPO nunmehr die Verpflichtung des Abbruchs der Überwachung auf alle berufsgruppenbezogenen Vertrauensverhältnisse im Sinne des § 53 StPO. Das Stimmungsbild wird jedoch wohl auch durch die Sicht bestimmt, dass die Erweiterung des Journalistenschutzes des Jahres 2002 nicht unbedingt in das Bild der Welt nach dem 11. September 2001 passt.[278]

Die Rechtsprechung des Bundesverfassungsgerichts verweist darauf, dass es verfassungsrechtlich nicht gefordert ist, Medienvertreter grundsätzlich aus der Telekommunikationsüberwachung auszunehmen.[279] Das Bundesverfassungsgericht hat auch erklärt, dass einem unbehelligten telefonischen Kontakt zu gesuchten Straftätern verfassungsrechtlich grundsätzlich ein geringeres Gewicht zukomme als das Interesse an der Kommunikation mit Personen, die als Informanten den Medien für die Öffentlichkeit wichtige Informationen zukommen lassen, etwa zur Aufdeckung und Aufklärung von Missständen. Jedoch ist die grundrechtlich geschützte Pressefreiheit im Rahmen der Verhältnismäßigkeitsprüfung angemessen zu gewichten. Freilich ist zu bezweifeln, ob diese besondere Verhältnismäßigkeitsprüfung den Anforderungen des Europäischen Gerichtshofs für Menschenrechte standhält, die dieser an nationale Rechtsordnungen für den Fall der Telekommunikationsüberwachung von zeugnisverweigerungsberechtigten Berufen stellt.[280]

Auch aus diesem Grunde erscheint es – wenn auch nicht verfassungsrechtlich gefordert – angemessen, die Regelungen der verdeckten Ermittlungsmaßnahmen im Hinblick auf den Schutz der Zeugnisverweigerungsrechte (und der dahinter stehenden Interessen) zu harmonisieren und für § 100h II StPO ebenso wie für § 100a StPO eine der Lösung für die akustische Wohnraumüberwachung vergleichbare Regelung vorzusehen. Von ebenso großer Bedeutung ist freilich die Transparenz in der Durchführung von Strafverfahren (mit und ohne verdeckte Ermittlungsmaßnahmen) gegen Journalisten (und andere Berufe). Hierzu gehört eine besondere Erfassung und Auswertung von eingeleiteten Ermittlungsverfahren, die die Presse betreffen. Nur so wird auch systematisch (und nicht bloß punktuell[281]) überprüft werden können, wie der Verhältnismäßigkeitsgrundsatz Beachtung findet.

Im Lichte dieser Erwägungen ist die Bundesregierung in Überlegungen eingetreten, die ein stimmiges Gesamtkonzept des Schutzes von Zeugnisverweigerungsberechtigten bei heimlichen Ermittlungsmaßnahmen zum Gegenstand haben[282]. Hierfür stand im Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (Bundestagsdrucksache 16/5846) zunächst § 53b StPO-E, der in der Fassung des am 1. Januar 2008 in Kraft getretenen Gesetzes als § 160a StPO enthalten ist.

XI. Kostentragung für die Verkehrsdatenabfrage

Wie bei §§ 100a, 100b StPO ist auch bei der Anwendung der §§ 100g, 100h StPO zwischen verschiedenen Arten von Kosten zu unterscheiden. Zum einen entstehen Kosten für die technischen Einrichtungen zur Umsetzung der Maßnahmen sowie die fortlaufende Pflege und zum anderen im Einzelfall durch die Abfrage der Daten und die Auskunftserteilung gegenüber den Polizei- und Justizbehörden.

Inwieweit die Dienstanbieter für den Einsatz der elektronischen Datenverarbeitung im Rahmen der Auskunftserteilung zu Verkehrsdaten entschädigt werden, ist gesetzlich nicht ausdrücklich geregelt. In § 110 I Satz 1 Nr. 1 TKG ist allgemein festgelegt, dass die Kosten für die technischen Einrichtungen zur Umsetzung gesetzlicher Maßnahmen von den Telekommunikationsunternehmen selbst zu tragen sind (so auch §§ 110 IX Satz 2 TKG, 113 II Satz 1 TKG). Eine analoge Anwendung des § 23 III, IV JVEG, der die Entschädigung bei Rasterfahndungen regelt, kommt nach verschiedenen obergerichtlichen Entscheidungen nicht in Betracht.[283] In Bezug auf die Kosten für die Umsetzung der Maßnahmen nach §§ 100a, 100b StPO und § 113 TKG ist in § 110 IX TKG vorgesehen, dass eine Rechtsverordnung zur Regelung einer angemessenen Entschädigung erlassen werden darf. Die §§ 100g, 100h StPO werden dort nicht genannt.[284] Von der Möglichkeit des Erlasses einer Rechtsverordnung hat die Bundesregierung bisher keinen Gebrauch gemacht. Weitere Kostenregelungen finden sich in §§ 112, 113 TKG. Diese beziehen sich allerdings nur auf Bestandsdaten.

Die Kostentragungspflicht der Telekommunikationsunternehmen ist bei der Abfrage im automatisierten Verfahren ausdrücklich geregelt (§ 112 V TKG). Im Rahmen der manuellen Abfrage lässt § 110 IX TKG den Erlass einer Rechtsverordnung zur Regelung der Entschädigung zu.

---

[277] Vgl. BVerfGE 77, S. 65 ff; BVerfG NJW 2003, S. 1787.
[278] *Kunert*, NStZ 2002, S. 174.
[279] BVerfG NJW 2003, S. 1787.
[280] Rspr.-übersicht und Analyse bei *Esser,* 2002, S. 159 f.
[281] Wie in Überprüfungen durch Gerichte, vgl. hierzu beispielsweise BVerfG, Urteil vom 2. März 2006 – 2 BvR 2099/04.
[282] Bundesratsdrucksache 702/01, S. 11; Bundestagsdrucksache 14/7008, S. 8.
[283] OLG Köln NStZ-RR 2001, S. 31 f.; OLG Stuttgart, NStZ 2001, S. 158.
[284] *Bock*, in: Beck’scher TKG-Kommentar, 2006, § 110 Rn. 113.

Da eine solche Rechtsverordnung allerdings noch nicht vorliegt, sind die Telekommunikationsanbieter gemäß § 23 I Satz 1 Nr. 2 JVEG wie Zeugen (§ 19 JVEG) zu entschädigen.

Ebenso verhält es sich bei den Verkehrsdaten. Die dafür anfallenden Kosten sind nach dem JVEG abzurechnen.[285] Gemäß § 23 I Satz 1 Nr. 2 JVEG sind die Diensteanbieter auch hier wie Zeugen (§ 19 JVEG) zu entschädigen. Nach § 23 II JVEG werden dabei Aufwendungen für den notwendigen Einsatz eigener Arbeitnehmer als sonstige Aufwendungen nach § 7 I Satz 1 JVEG ersetzt. Eine Notwendigkeit des Einsatzes von Arbeitnehmern ist bei Unternehmen wie Telekommunikationsanbietern immer anzunehmen.[286] Der Höchstbetrag, der ersetzt wird, liegt nach § 22 I JVEG bei 17 Euro pro angefangene Stunde. Gemäß § 19 II S. 1 JVEG ist die Entschädigung auf zehn Stunden je Tag begrenzt. Die zu ersetzenden Kosten fallen dem Staat zur Last. Die Verteilung der Auslagen auf die beteiligten Behörden richtet sich nach den jeweiligen Landesverwaltungsvorschriften.[287]

Entschädigt werden die Telekommunikationsunternehmen allein für die durch konkrete Überwachungsmaßnahmen, etwa für Einzelauskünfte über Verkehrsdaten, anfallenden Kosten.[288] Die Zuarbeit für die Strafverfolgungsbehörden erfordert auch im Rahmen der Verkehrsdatenabfrage, für die die TKÜV nicht gilt, organisatorische, personelle und sachliche Investitionen, die nach der geltenden gesetzlichen Regelung nicht vollständig ausgeglichen werden.[289] Im April 2005 wurde im Rahmen des Gesetzgebungsverfahrens zur TKG Novelle 2005 ein Änderungsantrag der Fraktionen SPD und Bündnis 90/Die Grünen mit dem Entwurf eines neu einzufügenden § 113a TKG-E eingebracht[290], in dem eine pauschale (und auch Investitionskosten umfassende) Entschädigung für die Telekommunikationsüberwachung nach §§ 100a, 100b, 100g, 100h StPO vorgeschlagen wurde. Begründet war der Vorschlag mit der Erbringung von im staatlichen Verantwortungsbereich liegenden Leistungen (Strafverfolgung) sowie mit dem rechtspolitischen Ziel, den Gebrauch der Telekommunikationsüberwachung zu dämpfen. Der Vorschlag fand jedoch keine Zustimmung.

Ob die Verpflichtung, Infrastruktur für die Telekommunikationsüberwachung vorzuhalten, ohne angemessene Entschädigung verfassungsrechtlich zulässig ist, ist umstritten.[291] Zur Begründung der Kostentragungspflicht der Telekommunikationsanbieter wird vorgetragen, die Unterstützung der Strafverfolgung sei als *Sonderopfer* oder Sonderabgabe für die Interessen der Allgemeinheit anzusehen.[292] Demnach sind private Unternehmen verpflichtet, im öffentlichen Interesse ein Sonderopfer zu erbringen. Freilich setzt die Erhebung einer Sonderabgabe nach der Rechtsprechung des Bundesverfassungsgerichts eine spezifische Beziehung zwischen dem Kreis der Abgabenpflichtigen und dem mit der Abgabenerhebung verfolgten Zweck voraus.[293] Betont wird dabei die Bedeutung der besonderen inhaltlichen Nähe zwischen einem privaten Sektor und der mit einem Sonderopfer verfolgten Ziel für die Begründetheit der Erhebung einer Sonderabgabe.[294] Ein solcher Zusammenhang kann aber zwischen Telekommunikationsunternehmen und dem Interesse der Strafverfolgung nicht sofort gesehen werden. Telekommunikationsunternehmen stehen dem Zweck der Strafverfolgung nicht näher als andere private Sektoren[295], sieht man davon ab, dass durch Veränderungen in Technik und menschlicher Kommunikation dort in besonderem Maße Daten anfallen, die partiell (freilich zu einem verschwindend geringen Teil) zur Strafverfolgung genutzt werden können. Bei der Strafverfolgung handelt es sich um eine zentrale staatliche Aufgabe, für die keine besondere Sach- und Verantwortungsnähe der Diensteanbieter angenommen werden kann.[296] Die Erfüllung der von den Anlagenbetreibern verlangten Aufgaben steht zudem ausschließlich im Interesse der Allgemeinheit.[297] Für die Telekommunikationsunternehmen folgt aus der Durchführung von Telekommunikationsüberwachungsmaßnahmen kein für den Geschäftsbetrieb relevanter Nutzen.[298] Soweit die Aufklärung von Straftaten bezweckt ist, die mit der Telekommunikation in keiner funktionalen Beziehung stehen, sind insoweit die gewünschten Verkehrsdaten Beweismittel wie andere, deren Beschaffung grundsätzlich auf staatliche Kosten zu erfolgen hat.[299]

Ein weiterer Anknüpfungspunkt wird in der Literatur im Zurechnungsprinzip gesehen. Die Pflicht zur aktiven Abwehr von missbräuchlicher Nutzung bereitgestellter Technik und anderer Leistungen ergibt sich danach aus gewerblichen Standespflichten sowie aus einer erweiterten und allgemeinen staatsbürgerlichen Pflicht, die staatliche Strafverfolgung nicht zu vereiteln. Verantwortlichkeit bestehe darüber hinaus aber auch dafür, Strafverfolgung zu ermöglichen. Die Strafverfolgung kann zwar nicht – wie jedenfalls teilweise die Gefahrenabwehr – als private Aufgabe verstanden werden; ausweislich § 258 StGB dürfen Private die Aufklärung von Delikten nicht verhindern.[300] Verantwortlichkeit wird demnach für den durch das Gewerbe beschriebenen Risikobereich zugewiesen. Die Verantwortlichkeit entsteht nach dieser Auffassung aus der Beherrschung eines spezifischen Risikobereichs. Hier wird denn auch eine Pflicht gesehen, dafür zu sorgen, dass ein Gewerbe nicht voraussehbar für sozialschädliche Zwecke missbraucht werde.[301] In der Regel haftet ein Unternehmen zwar nur für Schäden aus dem bestimmungs-

---

[285] *Bock*, in: Beck´scher TKG-Kommentar, 2006, § 110 Rn. 113.
[286] *Zimmermann*, 2005, § 23 Rn. 12.
[287] Vgl. BW Verwaltungsvorschrift des Innenministeriums über die Auslagen der Polizei in Straf- und Bußgeldverfahren, GABl. 1995, S. 303, 305.
[288] *Dorsch*, 2005, S. 31 f.
[289] *Königshofen,* in: BKA (Hrsg.), 2004, S. 79.
[290] Bundestagsausschussdrucksache 15 (9) 1867, S. 1 f.
[291] Vgl. zur Vereinbarkeit mit der Europäischen Menschenrechtskonvention zusammenfassend *Breyer*, European Law Journal, 2005.
[292] *Schmidt-Preuß*, 2005, S. 3.
[293] BVerfGE 55, S. 274, 306.
[294] BVerfGE 55, S. 274, 307.
[295] *Dorsch*, 2005, S. 37.
[296] *Hammerstein*, MMR 2004, S. 225.
[297] *Hammerstein*, MMR 2004, S. 225; *Kube/Schütze*, CR 2003, S. 669.
[298] *Kube/Schütze,* CR 2003, S. 669.
[299] *Welp*, 2000, S. 137.
[300] *Waechter*, VerwA 1996, S. 90.
[301] *Waechter*, VerwA 1996, S. 90.

gemäßen Gebrauch von Produkten oder Anlagen. Jedoch unterbricht auch eine bestimmungsfremde Verwendung von Gegenständen nicht stets den Zurechnungszusammenhang. Bezug genommen wird auf die für die Produkthaftung anerkannte Regel, dass auch für Schäden aus bekannten und üblichen missbräuchlichen Verwendungen Ersatz zu leisten ist.[302] Gegen eine Zurechnung wird vorgebracht, dass bei absichtlichem Missbrauch von Anlagen oder Produkten durch Dritte weder eine Pflichtwidrigkeit vorliege, noch die Gefährdung aus dem Verantwortungsbereich eines Unternehmens stamme.[303] Stattdessen seien entweder die Dritten als Störer oder die Allgemeinheit wegen der Schaffung und Akzeptanz kriminogener Strukturen moderner Gesellschaften verantwortlich.[304]

Schließlich wird in der Literatur[305] für repressive Maßnahmen eine Differenzierung entsprechend der für präventive Maßnahmen in den *Polizeigesetzen der Länder* geltenden Kategorien der Zustands-, Handlungs- und Nichtstörer vorgeschlagen. Danach würde die Verpflichtung zur Kostenübernahme davon abhängen, ob Telekommunikationsunternehmen als Zustandsverantwortliche oder als Nichtstörer einzustufen sind. Wer aber als Nichtverantwortlicher durch eine polizeirechtliche Maßnahme belastet wird, erhält hierfür einen Ausgleich.[306] Eine Verpflichtung ohne Entschädigung wäre dann rechtswidrig.

Die Forderung einer aufwandsadäquaten Entschädigung für die Beiziehung zu Telekommunikationsmaßnahmen wird schließlich auf die Wahrung der Verhältnismäßigkeit bei Eingriffen in die Berufs- und Eigentumsfreiheit gestützt.[307]

Anlässlich der Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung forderte der Bundestag in einem Antrag die Bundesregierung dazu auf, zeitnah einen Gesetzesentwurf für eine angemessene Entschädigung der Telekommunikationsunternehmen für die Inanspruchnahme im Rahmen der Erfüllung hoheitlicher Ermittlungsmaßnahmen im Bereich der Telekommunikation vorzulegen.[308] Dem ist die Bundesregierung bisher nicht nachgekommen. Im am 1. Januar 2008 in Kraft getretenen Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen (Bundesgesetzblatt 2007. I, Nr. 70, S. 3198) ist dies ausdrücklich nicht vorgesehen. Jedoch wurde ein gesonderter, alsbald vorzulegender Gesetzentwurf mit Entschädigungsregelungen angekündigt.

[302] *Waechter*, VerwA 1996, S. 91.
[303] *Waechter*, VerwA 1996, S. 88.
[304] *Waechter*, VerwA 1996, S. 88.
[305] BVerwG mit Anmerkung *Karpen*, JZ 1986, S. 896 ff.; BVerwG mit Anmerkung *Karpen*, JZ 1989, S. 895, 899.
[306] *Kube/Schütze*, CR 2003, S. 669.
[307] *Günther*, Kriminalistik 2004, S. 16; *Günther*, in: BKA (Hrsg.), 2004, S. 69. *Eckhardt*, CR 10/2001, S. 675; *Königshofen,* in: BKA (Hrsg.), 2004, S. 79; *Kube/Schütze*, CR 2003, S. 671; *Bock*, in: Beck'scher TKG-Kommentar, 2006, § 110 Rn. 17; *Schmidt-Preuß*, 2005, S. 29; BDI-Positionspapier, „Telekommunikationsüberwachung verfassungsgemäß und wirtschaftsfreundlich gestalten" vom 7. Oktober 2003, S. 2, http:/www.bdi-online.de; *Wu*, 2005, S. 147.
[308] Bundestagsdrucksache 16/545, S. 4.

Der österreichische Verfassungsgerichtshof hat im Jahre 2003 entschieden, dass die der deutschen Regelung entsprechende Normierung in § 89 I TKG (Österreich) verfassungswidrig ist.[309] Nach der österreichischen Vorschrift waren die Betreiber u. a. dazu verpflichtet, auf eigene Kosten alle Einrichtungen bereitzustellen, die zur Überwachung des Fernmeldeverkehrs erforderlich sind (§ 89 I TKG-Österreich). Ein Kostenausgleich war nur für die Mitwirkung an einzelnen Überwachungsmaßnahmen vorgesehen (§ 89 II TKG-Österreich). Dies entspricht der jetzigen deutschen Regelung. Der Österreichische Verfassungsgerichtshof begründete die Verfassungswidrigkeit der Regelung mit der Unverhältnismäßigkeit eines vollständigen Ausschlusses von Kostenersatz für die erheblichen Investitionen in die technische Realisierung und Installation der Einrichtungen zur Überwachung.[310] Jedenfalls dürfen nach den Ausführungen des Österreichischen Verfassungsgerichtshofs die bei Erfüllung staatlicher Aufgaben anfallenden Kosten (der Infrastruktur) nicht vollständig auf private Unternehmen abgewälzt werden. Diese Erwägungen sind grundsätzlich auf die deutsche Rechtslage übertragbar.[311]

XII. Vorratsdatenspeicherung

Gegenstand aktueller rechtspolitischer Diskussionen ist vor allem die Einführung der Vorratsdatenspeicherung. Die Richtlinie RL 2006/24/EG verlangt von den Mitgliedsländern der Europäischen Union eine einheitliche Gesetzgebung zur Speicherung von Telekommunikationsverkehrsdaten für mindestens sechsund höchstens 24 Monate.

Das geltende Recht verpflichtet die Anbieter nur zur Erfassung der Bestandsdaten, nicht aber zur Speicherung der Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung. § 96 II Satz 1 TKG begrenzt die Speicherung von Verkehrsdaten auf den Zweck des Aufbaus von Verbindungen, das Ziel der Entgeltermittlung und Entgeltabrechnung, für die Erstellung eines Einzelverbindungsnachweises und die Erkennung bzw. Beseitigung von Störungen von Telekommunikationsleistungen oder des Missbrauchs von Telekommunikationsdiensten. Dies entspricht den Vorgaben, die aus Datenschutzrichtlinien und weiteren europäischen Instrumenten folgen. Nach Versendung der Rechnung dürfen die Verkehrsdaten höchstens für sechs Monate gespeichert werden (§ 97 III Satz 3 TKG). Im Übrigen sind die Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen (§ 96 II Satz 2 TKG). Für die Daten der Angerufenen sieht § 96 III Satz 2 TKG eine Anonymisierungspflicht vor.

[309] Österreichischer VfGH v. 27. Februar 2003, Az. G37/02, S. 2.
[310] Österreichischer VfGH v. 27. Februar 2003, Az. G37/02, S. 44.
[311] Vgl. im Übrigen *Kilchling* 2008, wo in einem für den Verband der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM) erstellten Gutachten zu „Die Neuregelung zur Auslandkopfüberwachung gemäß § 4 TKÜV auf dem verfassungsrechtlichen Prüfstand" davon ausgegangen wird, dass die geltenden Kostenregelungen verfassungswidrig sind.

Diese Speichermöglichkeiten waren in jüngerer Vergangenheit durch die Rechtsprechung freilich deutlich eingeschränkt worden, und zwar für diejenigen Telekommunikationsvorgänge, für die (nächträgliche) Einzelabrechnungen nicht anfallen. Dies betrifft zum einen die Verkehrsdaten über Verbindungen mittels Prepaid-Karten. Für diese Fälle hat das Bundesverfassungsgericht eine Speicherung durch die Telekommunikationsunternehmen als Eingriff in das Grundrecht des Nutzers aus Artikel 10 I GG bejaht, da ein verfassungsrechtlich anerkennenswertes Interesse an einer Datenspeicherung in diesen Fällen mangels Rechnungserstellung überhaupt zweifelhaft sein. Die Eingriffsqualität der Speicherung ergibt sich für das Gericht vor allem aus der mit der Speicherung verbundenen – abstrakten – Missbrauchsgefahr durch das Telekommunikationsanbieter selbst oder Dritte sowie die Möglichkeit staatlicher Zugriffe aufgrund von § 100 g StPO.[312] Ähnliche Bedenken haben zuvor den Bundesgerichtshof dazu bewogen, T-Online die Speicherung der Internet-Verkehrsdaten bei Nutzern von Flatrates zu untersagen.[313] In Folge der beiden Entscheidungen sind T-Com und andere Provider offensichtlich dazu übergegangen, die Verkehrsdaten in diesen Fällen nur noch für einen Zeitraum von sieben Tagen zu speichern.[314] Diese Nutzerkreise werden durch die Vorratsdatenspeicherung erneut betroffen.

Die zitierten Entscheidungen verweisen insbesondere auf eine erweiterte Datensicherheitsproblematik. Tatsächlich eröffnen sich im Hinlick auf die zusätzlichen Datenbestände neue Missbrauchsgefahren. Denkbar sind sowohl Missbrauch von innen als auch unberechtigte Zugriffe von außen. Die Einrichtung der notwendigen Schnittstellen wird weiteres organisatorisches und personelles Datenschutzmanagement erfordern, das neu zu den oben erörterten Kostenposten hinzutreten wird.

Diskussionen um die Einführung einer Vorratsspeicherung und Mindestspeicherfrist werden in Deutschland ebenso wie in anderen Ländern der Europäischen Union seit einigen Jahren geführt. Sowohl im Jahre 2002[315] als auch 2003[316] kam es zu Bundesratsinitiativen für die Einführung der Vorratsspeicherung, die jedoch keine Mehrheit fanden. Die Bundesratsinitiativen waren mit der Verbesserung der Effizienz strafrechtlicher Ermittlungen begründet. Befürchtet wurde, dass die Verkehrsdatenabfrage, soweit die betroffenen Daten nicht mehr vorhanden sind, ins Leere läuft.[317] Der Bundestag hat sich in Stellungnahmen gegen eine Mindestspeicherfrist ausgesprochen.[318] Er führte dazu aus[319], dass gesetzliche Löschungspflichten zwar im Einzelfall den Zugriff von Strafverfolgungsbehörden auf für sie relevante Daten verhindern könnten. Eine präventive generelle Speicherung von Telekommunikationsverkehrsdaten würde jedoch die Bildung von Persönlichkeitsprofilen erheblichen Ausmaßes zulassen. Es bedürfe daher einer genauen Prüfung, ob eine derart umfassende Speicherung angemessen ist. Zudem entstünde ein erheblicher Aufwand und es bleibe ungewiss, ob die Daten für den mit der Speicherung verfolgten Zweck tatsächlich irgendwann einmal benötigt würden.[320] Eine allgemeine Vorratsdatenspeicherung wurde vom Bundesverfassungsgericht insbesondere in der Entscheidung zum Volkszählungsgesetz als besonderes Problem aufgegriffen. Eine „Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken“, so der Tenor der Rechtsprechung des Bundesverfassungsgerichts bis heute, ist wegen eines unverhältnismäßigen Eingriffs in das Recht auf informationelle Selbstbestimmung verfassungswidrig.[321] Der Gesetzgeber ist angehalten, den Verwendungszweck bereichsspezifisch und präzise zu bestimmen, und die Speicherung auf solche Daten zu beschränken, die für den verfolgten Zweck geeignet und erforderlich sind.[322]

Die EU-Richtlinie sieht vor, dass Telekommunikations-Verkehrsdaten künftig mindestens sechs und höchstens 24 Monate lang für Zwecke der Strafverfolgung und der Gefahrenabwehr gespeichert werden. Dies soll gemäß Artikel 1 der Richtlinie der Harmonisierung der Vorschriften der Mitgliedstaaten über die Regelung der Vorratsdatenspeicherung dienen und vor allem vergleichbare wirtschaftliche Rahmenbedingungen für Telekommunikationsunternehmen schaffen. Freilich steht im Hintergrund die Überzeugung, dass präventive und repressive Bedürfnisse vor allem der Terrorismusbekämpfung nach einer allgemeinen Speicherung von Verkehrsdaten in Europa verlangen.

Am 16. Februar 2006 hat der Deutsche Bundestag einen Antrag zur sechsmonatigen Speicherung von Telefon- und Internetdaten beschlossen. Die Bundesregierung ist damit aufgefordert, die vom Europäischen Parlament angenommene Richtlinie zur Aufzeichnung der Nutzerspuren umzusetzen. Der Bundestag forderte in diesem Antrag die Bundesregierung auch dazu auf, zeitnah einen Gesetzesentwurf für eine angemessene Entschädigung der Telekommunikationsunternehmen für die Inanspruchnahme im Rahmen der Erfüllung hoheitlicher Ermittlungsmaßnahmen im Bereich der Telekommunikation vorzulegen.[323] Weiter wurde darauf hingewiesen, dass bei der Umsetzung der Richtlinie nicht über die Mindestanforderungen der Richtlinie hinsichtlich Speicherungsdauer und Art der erfassten Daten hinausgegangen werden soll.

Die Bundesregierung hat dann am 18. April 2007 einen Gesetzesentwurf zur Neuregelung der Telekommunika-

---

[312] BVerfG, 1 BvR 1811/99 vom 27. Oktober 2006, MMR 2007, S. 308.
[313] BGH, III ZR 40/06 vom 26. Oktober 2006, MMR 2007, S. 37.
[314] Vgl. www.heise.de/newsticker/meldung/85609.
[315] Bundesratsdrucksache 275/02 v. 31. Mai 2002; Bundestagsdrucksache 14/9801, S. 14 v. 17. Juli 2003.
[316] Bundesratsdrucksache 755/03, S. 33 (Stellungnahme des Bundesrates vom 19. Dezember 2003).
[317] Bundesratsdrucksache 755/03, S. 34 (Stellungnahme des Bundesrates vom 19. Dezember 2003).
[318] Bundestagsdrucksache 14/9801, S. 15; Bundestagsdrucksache 15/4597, S. 3.
[319] Bundestagsdrucksache 14/9801, S. 15.
[320] Bundestagsdrucksache 14/9801, S. 16.
[321] BVerfGE 65, S. 1, 46.
[322] BVerfGE 65, S. 1, 46.
[323] Bundestagsdrucksache 16/545, S. 4.

tionsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vorgelegt[324], der auch der Umsetzung der Europäischen Richtlinie dient und die Vorratsdatenspeicherung berücksichtigt. Die Reform ist am 1. Januar 2008 in Kraft getreten. Danach legt § 113a TKG fest, dass jeder Diensteanbieter verpflichtet ist, bestimmte von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten für die Zwecke der Strafverfolgung sechs Monate lang zu speichern. Gespeichert werden nach II die Rufnummern des anrufenden und des angerufenen Anschlusses sowie die Rufnummern, an die der Anruf weitergeleitet wird, Beginn und Ende der Verbindungen sowie Angaben zu dem jeweils genutzten Dienst. Im Fall mobiler Telefondienste ist ferner die Speicherung der Kennung der Mobilfunkkarte des anrufenden oder angerufenen Anschlusses, der Kennung des anrufenden und des angerufenen Endgerätes und der Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen vorgesehen.

Für Internettelefondienste wird die Internetprotokolladresse des anrufenden und des angerufenen Anschlusses registriert. E-Mail-Adressen, IP-Adressen des Absenders der übermittelten Nachricht, Beginn und Ende der Nutzung des Dienstes sind ebenfalls zu erfassen. Schließlich werden die IP-Adresse des Teilnehmers für eine Internetnutzung, die Kennung des Anschlusses, über die die Internetnutzung erfolgt, sowie Beginn und Ende der Internetnutzung festgehalten. Daten, die Aufschluss über den Inhalt der Kommunikation oder angewählter Internetseiten geben, dürfen dagegen nicht gespeichert werden (Abs. 8). Schließlich soll die Speicherung so vorgenommen werden, dass Auskunftsersuchen der anfragenden Stellen unverzüglich beantwortet werden können (Abs. 9). Die Daten sind innerhalb eines Monats nach Ablauf der Speicherungsdauer von sechs Monaten zu löschen (Abs. 11).

§ 113b erlaubt die Weitergabe der nach § 113a TKG gespeicherten Daten nur für Zwecke der Strafverfolgung, zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist. Entsprechende Regelungen existieren bislang weder zu präventiven Zwecken noch im Hinblick auf die genannten Dienste.

Die Verkehrsdatenspeicherung hat erhebliche rechts- und verfassungspolitische Kontroversen ausgelöst. Dies ist verständlich, geht es doch um strategische Abwägungen zwischen Sicherheit und dem Schutz des Privaten. Besondere Herausforderungen werden aus der Perspektive des Datenschutzes gesehen. Aus der Sicht von Datenschutzbeauftragten ist eine Vorratsdatenspeicherung, wie in der EU Richtlinie vorgesehen und in der am 1. Januar 2008 in Kraft getretenen Reform umgesetzt, deshalb verfassungswidrig[325], weil sie als anlassunabhängige und verdachtslose Überwachung des Telekommunikations- und Internetverkehrs einen unverhältnismäßigen Eingriff in Artikel 8 der EMRK bzw. des Fernmeldegeheimnisses mit sich bringe[326] und sich jedenfalls nicht sofort mit den Vorgaben des – allerdings lange zurück liegenden[327] – Volkszählungsurteils des Bundesverfassungsgerichts in Einklang bringen lasse. In der Beurteilung der Vorratsdatenspeicherung wird die Bedeutung des Telekommunikationsgeheimnisses als zentrales Menschenrecht in der Informationsgesellschaft betont und ferner darauf hingewiesen, dass Kommunikationsnetze nicht zu „Plattformen der Verdachtsschöpfung“ werden dürften.[328] Problematisch sei daher insbesondere auch die Zugriffsmöglichkeit der Nachrichtendienste.[329]

Als Alternative zur Vorratsdatenspeicherung wird zuweilen vorgeschlagen, das so genannte „Quick Freeze“ oder „Data Freeze“-Verfahren“ einzuführen.[330] Darunter versteht man ein (insbesondere in den USA praktiziertes und ferner in dem Übereinkommen des Europarats über Computerkriminalität enthaltenes) Verfahren, nach dem die Daten einer verdächtigen Person ab einem bestimmten Zeitpunkt auf richterliche Anordnung hin gespeichert und „eingefroren“ werden.[331] Jedoch geht es dabei im Kern lediglich um die derzeit geltende Verkehrsdatenabfrage, mit der ab dem Zeitpunkt der richterlichen Anordnung (oder staatsanwaltschaftlichen Eilentscheidung) auf entstehende Telekommunikationsverbindungen zugegriffen wird. Insoweit werden durch ein solches Verfahren eben gerade solche Daten nicht erfasst, auf die die Vorratsspeicherung abzielt, nämlich Daten, die aus betrieblichen Zwecken heraus nicht gespeichert werden und solche, die vor der in der Vorratsspeicherungsregelung vorgesehenen Frist gelöscht werden.[332]

Praktische Bedenken gegen die Vorratsspeicherung berufen sich auf Zweifel an der Kosten-Nutzen-Effizienz[333]

[324] Regierungsentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, Bundestagsdrucksache 16/5846.

[325] Vgl. auch *Sierck/Schöning/Pöhl*, 2006, S. 21.

[326] *Dix*, Kriminalistik 2004, S. 81.

[327] Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16. Februar 2006, S. 1428.

[328] *Dix,* in: BKA (Hrsg.), 2004, S. 164; vgl. ähnliche Erwägungen in Bundestagsdrucksache 16/237, S. 1.

[329] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Stellungnahme zum Gesetzentwurf der Bundesregierung Bundestagsdrucksache 275/07 vom 23. Augusst 2007, www.datenschutzzentrum.de/polizei/20070627-vorratsdatenspeicherung.htm, S. 26 f.

[330] Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16. Februar 2006, S. 1419; *Dix*, Kriminalistik 2004, S. 82.

[331] *Büllingen*, DuD 2005, S. 350; *Dix,* in: BKA (Hrsg.), 2004, S. 162; *Sierck/Schöning/Pöhl*, 2006, S. 14.

[332] Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16. Februar 2006, S. 1426; Commission Staff Working Document, Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, {COM(2005) 438 final}, Brüssel, 21. 9. 2005, S. 12; *European Working Party on Information Technology Crime,* 2001; Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16. Februar 2006, S. 1427

[333] Vgl. zu Kostenschätzungen *Larnhof,* 2006, S. 64f.; *Sierck/Schöning/Pöhl*, 2006, S. 14; Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16. Februar 2006, S. 1420.

und an der Beherrschbarkeit großer Datenmengen.[334] Zweifelhaft sei darüber hinaus, ob gegenwärtig überhaupt ein hinreichendes datenschutzrechtliches Regelungskonzept existiere, das den Gefahren einer missbräuchlichen Verwendung der Daten hinreichend vorbeugen könne.[335]

Irland hat im Juli 2006 vor dem EuGH (Nichtigkeits-) Klage gegen die Richtlinie erhoben. Die Irische Regierung vertritt die Auffassung, dass die Richtlinie als Rahmenbeschluss hätte erlassen werden müssen, nimmt freilich nicht zu substantiellen Fragen Stellung.[336] Irland war im Übrigen unter den ersten Mitgliedsländern der Europäischen Union, die eine Verpflichtung zur Verkehrsdatenspeicherung eingeführt haben. Auch der Deutsche Bundestag war zunächst der Ansicht, dass die Rechtsgrundlage in einem Rahmenbeschluss gesetzt werden müsse.[337] Gleichwohl wurde keine Nichtigkeitsklage von Seiten Deutschlands erhoben. Ein entsprechender Antrag zur Überprüfung der Richtlinie wurde abgelehnt.[338]

Dabei lassen die Implementationsdebatten in den Mitgliedsstaaten deutlich erkennen, dass tatsächlich Strafverfolgungs- und Datenschutzgesichtspunkte die Gesetzgebung maßgeblich bestimmen, und nicht so sehr (wenn überhaupt) genuin wirtschaftspolitische Überlegungen, wie bei einer EU-Richtlinie als Instrument zur Binnenmarktregulierung eigentlich zu erwarten wäre. Jedenfalls wird das ursprüngliche Ziel der Richtlinie, einheitliche Rahmenbedingungen für die Telekommunikationsunternehmen zu schaffen, angesicht des derzeitigen Stands der Umsetzung noch nicht erreicht (siehe Entwicklungen im Ausland).

C. Entwicklungen im Ausland

Die Abfrage von Telekommunikationsverkehrsdaten hat sich international zu einer Standardmaßnahme in strafrechtlichen Ermittlungen und bei der strategischen Informationsbeschaffung zu Zwecken der Gefahrenabwehr und -analyse entwickelt[339]. Dieser Prozess reflektiert die zunehmende Verbreitung von (mobilen) Telekommunikationsmitteln, die Digitalisierung und die hieraus resultierenden detaillierten und validen Informationen zu individuellem Verhalten sowie Beziehungsmustern. Rechtspolitische Debatten zur Nutzung von Verkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr sind auch dadurch gekennzeichnet, dass für Verkehrsdaten grundsätzlich von einer im Vergleich zu Kommunikationsinhalten weniger signifikanten Eingriffsintensität ausgegangen wird.

Kontroversen lassen sich im internationalen Vergleich insbesondere in der Behandlung des anonymen Zugangs zur Telekommunikation, der technischen Ausgestaltung der Verbindungen zwischen Strafverfolgungsbehörden und Telekommunikationsunternehmen (insbesondere unter Datenschutz- und Sicherheitsgesichtspunkten), der Kosten der durch den Ausbau der Überwachungsanforderungen bedingten Infrastrukturmaßnahmen in den Unternehmen sowie in der Frage der Vorratsspeicherung von Verkehrsdaten beobachten.

Betrachtet man die europäischen und außereuropäischen Entwicklungen, dann lässt sich auch feststellen, dass die Europäische Union bei der Einführung von Regelungen zur Verkehrsdatenspeicherung eine Vorreiterrolle spielt. Die Debatten um die Vorratsspeicherung haben sich auf Europa konzentriert.[340] Dies ist sicher eine Folge der Richtlinie 2006/24 und ihres etwa vierjährigen Entstehungsprozesses. Der Common Law Bereich, und hier die USA, Kanada und Neuseeland, hat sich bislang darauf beschränkt, anlassbezogene Regeln des Zugriffs auf Verkehrsdaten einzuführen bzw. den Zugriff auf Bestands- und Verkehrsdaten im Rahmen der Überwachung der Telekommunikation selbst zu nutzen.[341] In den USA hatten die Anschläge vom 11. September 2001 in Gestalt des Patriot Act 2001 zwar zu weitreichenden Erweiterungen der Exekutivbefugnisse auch in der Telekommunikationsüberwachung geführt. Jedoch sind die Verpflichtung zur Erfassung von Bestandsdaten und die Vorratsspeicherung von Verkehrsdaten zu diesem Zeitpunkt nicht ins Auge gefasst worden[342]; die anlassbezogenen Zugriffe auf Verkehrsdaten sind auf 90 Tage begrenzt, bei einer einmaligen Verlängerungsmöglichkeit um 90 Tage). 2006 lebte die Debatte über eine Verkehrsdatenspeicherung in den USA wieder auf, beschränkt auf Internetverbindungen und angefacht durch Fälle der Kinderpornografie sowie der sexuellen Ausbeutung von Kindern in online-Kommunikation über das Internet.[343] Ein Gesetzesantrag im Bundesstaat Colorado, der die Vorratsspeicherung für In-

---

[334] Bundestagsdrucksache 16/128, S. 2; siehe auch *Nuno Alvaro*, 2005, S. 3 f.

[335] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Stellungnahme zum Gesetzentwurf der Bundesregierung Bundestagsdrucksache 275/07 vom 23. August 2007, www.datenschutzzentrum.de/polizei/20070627-vorratsdatenspeicherung.htm, S. 28.

[336] *Sierck/Schöning/Pöhl*, 2006, S. 21; Pressemitteilung von Digital Rights Ireland vom 14. September 2006, abrufbar unter http://www.digitalrights.ie/2006/09/14/dri-brings-legal-action-over-mass-surveillance/.

[337] Bundestagsdrucksache 16/545, S. 3.

[338] Bundestagsdrucksache 16/1622: Antrag vom 26. Mai 2006 „Richtlinie zur Vorratsdatenspeicherung durch den Europäischen Gerichtshof prüfen lassen“; Plenarprotokoll 16/38 vom 20. Juni 2006, S. 3527D, Anlage 2.

[339] Vgl. hierzu die Nachweise in *Commission Staff Working Document*, Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, {COM(2005) 438 final}, Brüssel, 21. September 2005 sowie die Darstellung unter 1.D.III.

[340] In Argentinien wurde im Jahr 2004 eine Vorratsspeicherung für zehn Jahre eingeführt, kurz darauf aber wieder suspendiert, vgl. Decreto 357/2005: Suspéndese la aplicación del Decreto Nº 1563 del 8 de noviembre de 2004.
Suspéndese la aplicación del Decreto Nº 1563 del 8 de noviembre de 2004.

[341] Die größere Zurückhaltung deckt sich im Übrigen mit Umfrageergebnissen, nach denen die nordamerikanische Bevölkerung stärker als die kontinentaleuropäischer Länder am Schutz persönlicher Daten interessiert ist, vgl. hierzu *The Surveillance Project*, 2006, S. 11.

[342] *Crump,* Standford Law Review 2003.

[343] *Petersen*, EDUCAUSE Review 2006.

ternetverbindungen vorsah, fand im Jahr 2006 freilich im Parlament keine Mehrheit.[344]

In Kanada wurde anlässlich der Konsultationen zum Gesetz über die Modernisierung von Ermittlungstechniken (Modernization of Investigative Techniques Act, MITA, 2005) darauf hingewiesen, dass weder an die Einführung von „Know Your Customer“ Regeln noch von Verpflichtungen zur Speicherung von Bestands- oder Verkehrsdaten gedacht werde. Der Entwurf des Modernisierungsgesetzes MITA[345], mit dem die Umsetzung der Cyber Konvention des Europarats erfolgen sollte und das Telekommunikationsunternehmen verpflichtet hätte, die Kommunikationstechnik an Erfordernisse der Strafverfolgung anzupassen, fiel aus formellen Gründen 2005 aus dem Gesetzgebungsverfahren.[346] Voraussichtlich wird das Vorhaben in naher Zukunft wieder aufgegriffen.

In England/Wales wird der Zugang zu Telekommunikationsdaten (einschließlich Bestands- und Verkehrsdaten) in Teil I, Kapitel 2 des Gesetzes zur Regelung von Ermittlungsbefugnissen geregelt (RIPA, Regulation of Investigatory Powers Act 2000).[347] Der Zugang wird erlaubt für Polizeibehörden, Zoll, Geheimdienste und die Finanzbehörden. RIPA bezieht sich auf drei Arten von Telekommunikationsdaten: Verkehrsdaten, Nutzungsdaten und Nutzerdaten. Ein Code of Practice legt die Bedingungen fest, unter denen Angehörige der genannten Behörden auf diese Datenbestände zugreifen dürfen.[348] Die Polizei selbst (genau bestimmte Dienstgrade) hat das Recht, Abfragen anzuordnen. Bislang beruht die Speicherung der Verkehrsdaten freilich auf freiwilligen Vereinbarungen, die der Innenminister mit Telekommunikationsversorgern abschließen kann. Die Möglichkeit der Einführung zwingender Vorschriften sind in RIPA sowie im Anti-terrorism, Crime and Security Act 2001 angelegt. Für bestimmte Verkehrsdaten ist von den meisten Telekommunikationsfirmen in England eine Speicherung von zwölf Monaten vorgesehen. Insoweit wurden die Bedürfnisse der Strafverfolgungspraxis in Kombination mit RIPA bislang offensichtlich weitgehend erfüllt. Zum 1. Oktober 2007 werden die Data Retention (EC Directive) Regulations 2007 in Kraft treten, die in Umsetzung der EG Richtlinie 2006 die Pflicht zur Speicherung von Verkehrsdaten für einen Zeitraum von zwölf Monaten vorsehen.

In der Schweiz wurde durch das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs 2000 eine Speicherungspflicht mit einer Dauer von sechs Monaten eingeführt. Finnland und die Tschechische Republik streben derzeit ebenfalls eine der deutschen Regelung entsprechende Speicherungsdauer von sechs Monaten an. Schweden dürfte sich nach den bisherigen Überlegungen dem Sechs-Monatsmodell anschließen. Frankreich, Dänemark, Spanien und Belgien werden nach den bisherigen Plänen eine Speicherungsdauer von zwölf Monaten einführen oder haben dies bereits getan (Frankreich: Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques[349]; Spanien: Gesetzesentwurf 121/000128 Conservación de datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, vom 11. Juni 2007). Italien (Dekret 259/2003, „Codice delle comunicazioni elettroniche“, Dekret 196/2003, „Codice in materia di protezione dei dati personali, sowie das so genannte „decreto Pisanu“) und Irland haben bereits längere Speicherungsfristen implementiert, und zwar Italien mit einer Dauer von zwei Jahren (mit Verlängerungsmöglichkeit bis zu vier Jahren für Telefondaten, Internetverbindungsdaten: sechs Monate) und Irland von drei Jahren (allerdings ebenfalls begrenzt auf Telefonverbindungsdaten; Irish Criminal Justice (Terrorist Offences) Act, 2005).

In den Niederlanden steht derzeit ein Gesetzesentwurf zur Umsetzung der Europäischen Richtlinie in der Diskussion, nach dem eine Speicherungszeit für Telefon- und Internetverbindungsdaten von 18 Monaten eingeführt werden soll. Die Vorlage ist vom niederländischen Datenschutzbeauftragten kritisch gewürdigt worden, der unter Berufung auf neuere Stellungnahmen der Artikel 29 Arbeitsgruppe[350] eine Orientierung am Minimum der EU Richtlinie für angemessen ansieht, im Übrigen aber ebenso wie die Europäischen Datenschutzbeauftragten bei der Vorratsspeicherung von Verkehrsdaten Artikel 8 der Europäischen Menschenrechtskonvention als berührt betrachtet.[351]

Die Umsetzung der Europäischen Richtlinie in Österreich hat zunächst zur Vorlage eines Entwurfs zur Änderung des Telekommunikationsgesetzes vom Juni 2007 geführt.[352] Eine Vielzahl von Stellungnahmen[353] hat dann eine Verschiebung der Behandlung des Entwurfs im Parlament und das Eingeständnis zur Folge gehabt, dass die Frist zur Umsetzung der Richtlinie (15. September 2007) nicht eingehalten werden wird. Der Entwurf sieht eine Speicherfrist von sechs Monaten vor. Das österreichische Bundesministerium für Inneres hat im Übrigen aus der Sicht der Sicherheitsbehörden dazu geraten, die Frist auf ein Jahr auszudehnen.

Insgesamt gesehen dürfte demnach im Prozess der Implementation der Europäischen Richtlinie ein Trend zur Vereinheitlichung der durch sicherheitspolitische Erwägungen begründeten Rahmenbedingungen der Telekommunikation (wie durch die Richtlinie beabsichtigt) nicht angelegt

[344] *Cyber Security Industries Alliance*, 2007.
[345] Zusammenstellung der Unterlagen aus dem Anhörungsverfahren in *Nevis Consulting Group Inc.*, 2003.
[346] Gilbert/Kerr/McGill, Criminal Law Quarterly 2007.
[347] *Walker/Akde*niz, Northern Ireland Legal Quarterly 2003.
[348] *Rowland,* The Journal of Information, Law and Technology 2004.

[349] Frankreich hat im Übrigen im Gesetz Nr. 2006-64 vom 23. Januar 2006 (relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers), Journal Officiel du 24 janvier 2006 mit dem Wegfall des Richtervorbehalts den Zugang zu Verkehrsdaten erleichtert (gebilligt durch das Verfassungsgericht, vgl. Conseil Constitutionelle**,** Décision n° 2005-532 DC vom 19. Januar 2006).
[350] Article 29 Arbeitsgruppe Opinion 3/2006 sowie Opinion 4/2005.
[351] *Opinion from the Dutch Data Protection Authority* (Dutch DPA) [College bescherming persoonsgegevens (CBP)] Legislative proposal (Bill) for implementation of the European Directive on Data Retention, Pertaining to the tender letter of 22 January 2007, S. 2.
[352] Entwurf: Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, 61/ME XXIII. GP.
[353] Einzusehen unter www.parlinkom.gv.at/portal/page?_pageid=908, 4662640&_dad=portal&_schema=PORTAL.

sein. Unsicherheit und Unterschiede werden deutlich, wenn die Zielsetzung der Schaffung gleicher Rahmenbedingungen für den Wettbewerb der Telekommunikationsunternehmen in das Blickfeld rückt. Die wird gerade in der Behandlung von mit der Implementation der Vorratsspeicherung entstehenden Kosten sichtbar. Die englische Regelung von 2007 sieht in § 10 vor, dass das Innenministerium Kosten, die aus der Umsetzung der Vorratsspeicherung folgen, ersetzen kann. Die Übernahme der Kosten steht jedoch unter der Bedingung der Mitteilung der Kosten durch die Betreiberfirma und der Verständigung zwischen Unternehmen und Regierung über die Höhe der Aufwendungen. In Frankreich werden gestaffelte Tarife eingeführt (Artikel R. 213-1 Décret n° 2006-358 du 24 mars 2006), in die auch die mit der Implementation der Vorratsspeicherung verbundenen Kosten aufgenommen werden sollten. Damit hat die französische Gesetzgebung auf eine Entscheidung des Verfassungsgerichts reagiert, das im Jahr 2000 grundsätzlich festgestellt hat, dass der Staat die durch öffentliche Interessen begründete Verpflichtung zur Schaffung von Abhörkapazitäten in Telekommunikationsunternehmen nicht entschädigungslos setzen darf.[354] Der österreichische Entwurf stellt darauf ab, dass Mehrkosten nicht absehbar seien und enthält sich einer Regelung.[355] Das spanische Gesetz sieht vor, dass alle Kosten für Anpassungsmaßnahmen auf der Seite der Telekommunikationsunternehmen zu deren Lasten gehen.[356]

In den USA ist es im Zusammenhang mit CALEA (Regelung der Telekommunikationsüberwachung und der Verpflichtung der Telekommunikationsunternehmen, die Systeme an Überwachungsanforderungen anzupassen) zur Einrichtung eines Fonds gekommen, über den bis 2006 knapp 500 Millionen US-Dollar Investitionskosten (für Infrastrukturmaßnahmen) erstattet wurden.[357]

Ein Beispiel für das Modell der international wohl weit verbreiteten, vollständigen Abwälzung der Kosten für Infrastrukturanpassungsmaßnahmen auf Telekommunikationsunternehmen bietet die südafrikanische Gesetzgebung. Durch den „The Regulation of Interception of Communications and Provisions of Communication-related Information Act" aus dem Jahr 2002 werden neben der Pflicht zu einer zwölfmonatigen Speicherung der Verkehrsdaten alle damit verbundenen Kosten den Unternehmen auferlegt.

D. Forschungsstand zu Häufigkeit, Anwendungsstrukturen und den Folgen der Verkehrsdatenabfrage

I. Einführung

Der Forschungsstand zu der Verbreitung von Bestands- und Verkehrsdatenabfragen im Strafverfahren ist schon deshalb begrenzt, weil offizielle Statistiken zur Nutzung dieser Daten für Zwecke der Repression und Prävention nur selten zur Verfügung stehen. Ferner ist die empirische Forschung zu verdeckten und technischen Ermittlungsmethoden wenig entwickelt. Zwar ist seit dem 11. September das wissenschaftliche Interesse an Untersuchungen zu technischen Systemen der Überwachung erheblich angestiegen.[358] Empirische Untersuchungen konzentrierten sich dabei jedoch bislang ganz überwiegend auf die Videoüberwachung. Vor allem die Kommunikationsüberwachung in Strafverfahren ist international ein nur wenig beachtetes Forschungsfeld geblieben. Selbst zur Inzidenz der Bestands- und Verkehrsdatenabfrage werden lediglich punktuelle Einblicke möglich, die beispielsweise für die Niederlande die Abfrage von Bestandsdaten für das Jahr 2001 mit etwa 300 000 bis 350 000 Fällen angeben lassen.[359] Jedoch ist die Bedeutung von empirischen Daten zur Abfrage von Telekommunikationsverkehrs- und -bestandsdaten gerade in der Europäischen Richtlinie 2006/24/EG in Artikel 10 hervorgehoben worden. Die Mitgliedsländer der Europäischen Union sind dadurch angehalten, Grundinformationen zu den Abfragen in Statistiken zusammenzufassen. Dies soll ausweislich der Begründung, die im „Explanatory Report" enthalten ist, eine Grundlage für die für 2010 vorgesehene Evaluation der Maßnahme herstellen.[360]

Aus der Evaluationsperspektive ergeben sich verschiedene Fragestellungen, die einer empirischen Überprüfung grundsätzlich zugänglich sind. Hierzu gehören nicht nur Fragen nach Häufigkeit und Struktur der Abfrage von Verkehrsdaten selbst und deren Folgen für Ermittlungs- und Strafverfahren. Von Bedeutung sind auch Fragen nach dem Potential von Verkehrsdaten im Hinblick auf Beeinträchtigungen der Privatsphäre und effizienter Implementation von Sicherheitspolitik. Fragen nach allgemeinen Zusammenhängen zwischen Anonymität (oder verdeckter Kommunikation) und bestimmten Formen von Kriminalität haben besondere Bedeutung im Zusammenhang mit anonymen Prepaid-Zugängen zur Telekommunikation.[361] Die Politik der Unterbindung anonymer Telekommunikation durch die Implementation des „Know your Customer" Prinzips ist nach einer neueren Umfrage maßgeblich durch Sicherheits- und Kriminalitätskontrollerwägungen bestimmt.[362]

II. Entwicklungen in Telekommunikation und Telekommunikationsüberwachung

Im Bereich der Telekommunikations(inhalts)überwachung ist – wie in der Vergangenheit immer wieder kritisch hervorgehoben – ein kontinuierlicher Anstieg der Anordnungen festzustellen (vgl. Abbildung 1).

---

[354] Entscheidung Nr. 2000-441, DC vom 28. Dezember 2000.

[355] 61/ME XXIII. GP – Ministerialentwurf – Materialien, S. 1.

[356] Boletin Oficial de Las Cortes Generales, VIII LEGISLATURA, Serie A: PROYECTOS DE LEY 11 de junio de 2007 Núm. 128-9, S. 67.

[357] *Office of the Inspector General*, 2006; *Figliola*, 2007.

[358] *Marx*, Law and Social Inquiry 2006, S. 399 ff.

[359] *Kamerstukken* II 2001/02, 28 059, Nr. 3, S.17; geschätzt wurde eine Steigerung auf bis zu 900 000 Abfragen in den Folgejahren.

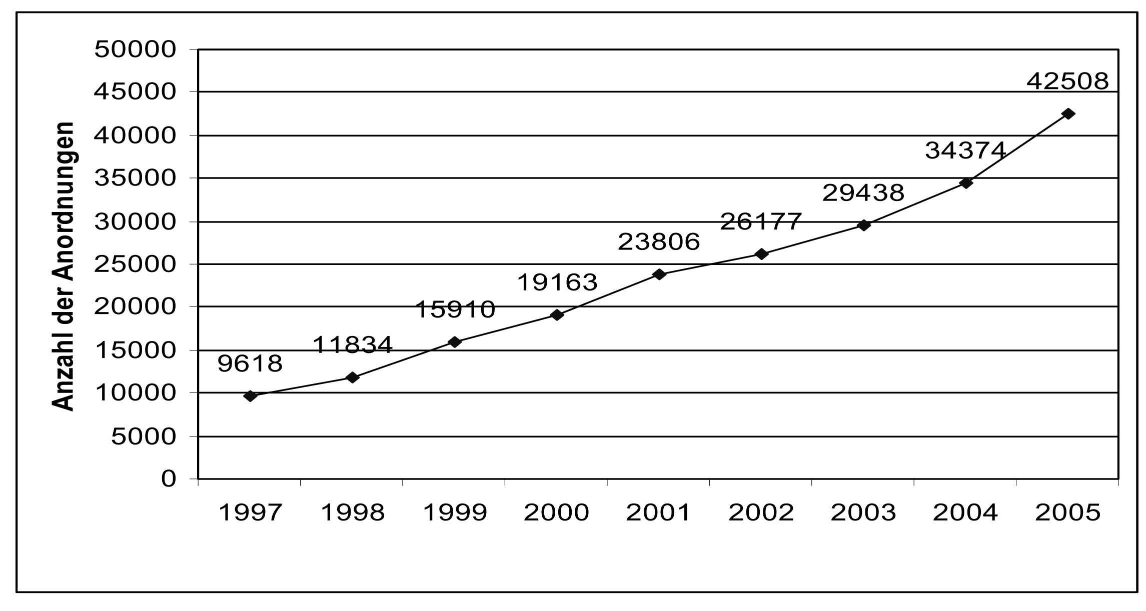
[360] Explanatory Report, zu Artikel 7.

[361] *Australian Privacy Foundation*, 2006, *Gow/Ihnat*, Surveillance & Society 2004.

[362] *Gow*, 2006.

Abbildung 1

Entwicklung der Telekommunikationsüberwachungsanordnungen von 1997 bis 2005 (mit Verlängerungen)



Quelle: Die Zahlen wurden von der Bundesnetzagentur zur Verfügung gestellt.

Von 9 618 Anordnungen nach §§ 100a, 100b StPO im Jahr 1997 steigt die Zahl auf 42 508 im Jahr 2005. Bestimmend für die Zunahme der Anordnungen im Bereich der Telekommunikationsüberwachungsmaßnahmen sind Veränderungen im Kommunikationsverhalten, die auch neue Rahmenbedingungen für polizeiliche Ermittlungen setzen. Bereits die Telekommunikationsüberwachungsstudie 2003 hat nachgewiesen, dass andere Erklärungen wenig plausibel sind.[363] Wie zeigt, hat sich der Mobilfunkverkehr erheblich ausgeweitet. Waren im Jahr 1990 noch 273 000 Mobilfunkgeräte angemeldet, so sind 2006 bereits 85 700 000 Mobiltelefone registriert. Demgegenüber bleibt die Anzahl der Festnetzanschlüsse nahezu konstant (z. B. 2002: 53,8 Mio. Telefonkanäle; 2006: 54,2 Mio. Telefonkanäle[364]). Seit 2004 ermöglicht zudem „Voice Over IP" das Telefonieren über das Internet. Allerdings macht die Internettelefonie mit 3,5 Mio. Telefonkanälen im Jahr 2006 bei insgesamt 142,3 Mio. Telefonkanälen nur einen sehr bescheidenen Anteil aus[365].

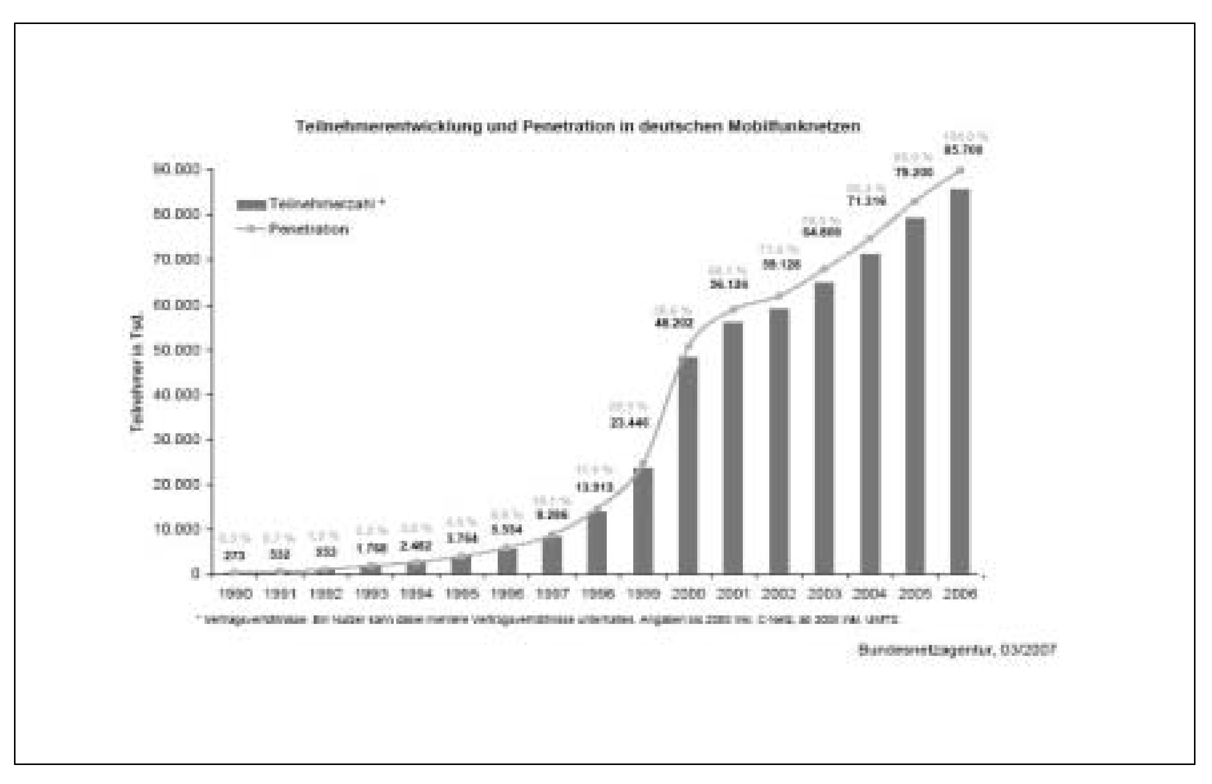
Ein anderes als das durch vermittelte Bild der Entwicklung der Telekommunikationsüberwachung und ihrer Dichte ergibt sich, wenn die Zahl der Mobiltelefone auf die Zahl der Telekommunikationsüberwachungsanordnungen bezogen wird. Wird die Zahl der verfügbaren Mobiltelefone als Bezugszahl genommen, dann zeigt sich, dass jedenfalls bis etwa zum Jahr 2000 die Dichte der Überwachung (gemessen anhand der einer Überwachungsanordnung gegenüberstehenden Zahl von Mobiltelefonen) drastisch sinkt. Während im Jahr 1997 auf knapp 900 Mobiltelefone eine Überwachung kam, betrug das Verhältnis im Jahr 2000 1: 2 500. In den Jahren nach 2000 nimmt die Überwachungsdichte jedoch wieder deutlich und offensichtlich in schnellem Tempo zu (2005: 1 : 1 863).

[363] *Albrecht/Dorsch/Krüpe*, 2003, S. 27 ff.
[364] *Bundesnetzagentur*, Jahresbericht 2006, S. 59.
[365] *Bundesnetzagentur*, Jahresbericht 2006, S. 59.

Abbildung 2



Entwicklung des Mobilfunkverkehrs



Quelle: Bundesnetzagentur, Jahresbericht 2006, S. 71 (in aktualisierter Fassung abrufbar unter http://www.bundesnetzagentur.de/media/archive/9040.pdf)

III. Umfang und Entwicklung der Verkehrsdatenabfrage

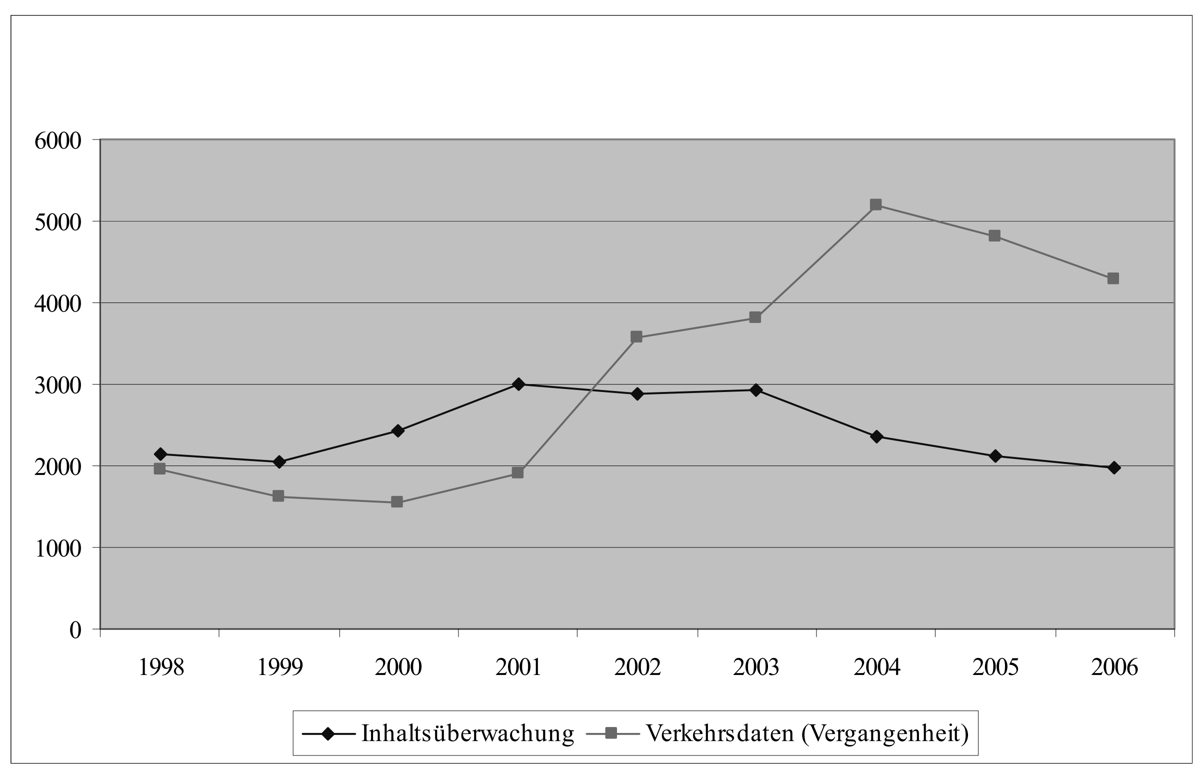
Im Gegensatz zu den Maßnahmen nach §§ 100a, 100b StPO wird über die Anzahl der Anordnungen nach §§ 100g, 100h StPO keine Statistik geführt. Weder die Justizbehörden noch die Telekommunikationsanbieter sind nach noch geltendem Recht dazu verpflichtet, die Anzahl der Anordnungen nach §§ 100g, 100h StPO statistisch zu erfassen.

Obwohl die Verkehrsdatenüberwachung im Vergleich zur Inhaltsüberwachung international als weniger belastend eingestuft wird, ist freilich die Bereitschaft, statistisches Material zu veröffentlichen, auch dort eher gering, wo, wie in den USA, detaillierte Berichte über die Telekommunikationsüberwachung regelmäßig vorgelegt werden. Statistiken zur Verkehrsdatenabfrage konnten nur für die Schweiz und für die USA identifiziert werden. Die beim Schweizer Amt für Besondere Ermittlungsmaßnahmen geführten Statistiken zur Telekommunikationsüberwachung zeigen, dass die Anzahl „rückwirkender Überwachungsmaßnahmen“ ab 2002 deutlich über den Zahlen der Überwachung der Kommunikationsinhalte liegt (Abbildung 3).[366]

[366] www.uvek.admin.ch/themen/kommunikation.

Abbildung 3

Verkehrsdaten- und Inhaltsüberwachung in der Schweiz



Quelle: www.uvek.admin.ch/themen/kommunikation

In den USA dürften bereits in den 1990er Jahren Verkehrsdatenabfragen sehr viel häufiger sein als die Inhaltsüberwachung der Telekommunikation.[367] Die dem Kongress jährlich berichteten, jedoch nicht veröffentlichten Daten zur Verkehrsdatenüberwachung unterscheiden zwischen so genannten „Pen Registers" (Erfassung ausgehender Verbindungen) sowie „Trap and Trace" (eingehende Verbindungen), die unter der (einfachen) Bedingung, dass sie für ein Ermittlungsverfahren relevant sein können, nach richterlicher Anordnung erhoben werden dürfen. Für 1998 wird die Zahl von 4 886 Anordnungen auf Bundesebene genannt (zuzüglich 4 621 Verlängerungen).[368] Unter Einschluss der einzelstaatlichen Ebene soll sich die Zahl in den 1990er Jahren bei etwa 10 000 Beschlüssen bewegt haben. Durch diese Zahlen werden allerdings andere Zugänge zu Verkehrsdaten in den USA nicht erfasst. Denn es besteht in den USA auch die Möglichkeit, Telekommunikationsfirmen über die (gerichtliche) Ladung als Zeugen (subpoena) zur Auskunft über Transaktionsdaten der Telekommunikation zu zwingen. Gerade dieser Zugang scheint weit verbreitet zu sein. Jedoch liegen über punktuelle Einblicke hinaus keine systematischen Erhebungen vor.[369]

Für England/Wales lässt sich aus einem Bericht über Überwachungsgesellschaften eine Information für das Jahr 2002 entnehmen. Danach haben Sicherheitsbehörden in diesem Zeitraum in etwa 400 000 Fällen Verkehrsdaten abgefragt.[370]

Aussagen über die Gesamtzahl der Beschlüsse oder der Abfragen zu unterschiedlichen Bereichen von Verkehrsdaten bzw. über Entwicklungen lassen sich auch für Deutschland auf der Grundlage einer einheitlichen Statistik nicht treffen. Im Zusammenhang mit der Stichprobenziehung der vorliegenden Untersuchung wurden jedoch die bei den einbezogenen Telekommunikationsanbietern verfügbaren internen Statistiken einer Auswertung unterzogen. Aus diesen Daten können Informationen zu Umfang, zur Struktur der Verkehrsdatenabfrage sowie zu Entwicklungen (zwischen 2002 und 2005) entnommen werden. Die Angaben der einzelnen Telekommunikationsanbieter beziehen sich jeweils nur auf die an sie gerichteten Beschlüsse. Eine einfache Addition der einzelnen Statistiken ist deshalb nicht möglich, weil die Beschlüsse nach §§ 100g, 100h StPO überwiegend auf mehr als einen Anbieter bezogen sind. Die Addition würde demnach zu überhöhten Werten führen. Darüber hinaus beziehen sich die Angaben einiger Anbieter nicht auf die Beschlüsse selbst, sondern auf die abgefragten

[367] www.wired.com/print/politics/security/news/2007/08/wiretap.
[368] www.wired.com/print/politics/security/news/2007/08/wiretap.
[369] www.cdt.org/wiretap/wiretap_overview.html: The Nature and Scope of Governmental Electronic Surveillance Activity, Juli 2006.

[370] *Ball/Murakami Wood*, 2006, S. 13.

Anschlüsse, wobei zum Teil weiter nach Art der Abfrage differenziert wird.

In der Aktenanalyse wurden beschlussbezogen die betroffenen Anbieter, die Anzahl der Anschlüsse und die Art der Abfrage erfasst. Auf der Grundlage dieser Informationen kann bestimmt werden, welcher Anteil der Beschlüsse sich jeweils auf einen Anbieter bezog und ob dabei eine bestimmte Art der Abfrage durchgeführt wurde bzw. wie viele Anschlüsse betroffen waren.

Damit wird es möglich, die Angaben der Unternehmen mit Hilfe der aus der Aktenanalyse bestimmten Anteile (Beschlüsse pro Unternehmen und ggf. Anzahl der Anschlüsse/Art der Abfragen) auf die Gesamtzahl der Beschlüsse nach §§ 100g, 100h StPO hochzurechnen. Allerdings sind in diesen Abschätzungen Unsicherheiten enthalten, die im Folgenden vorgestellt werden. Bei ca. 7 Prozent der Beschlüsse in der Aktenuntersuchung wurden die betroffenen Telekommunikationsanbieter nicht explizit benannt bzw. nur pauschal angegeben.[371] Obwohl in diesen Fällen nicht sicher ist, dass ein bestimmter Anbieter tatsächlich betroffen war, wurde angenommen, dass alle Anbieter abgefragt wurden. Dieses Verfahren führt dazu, dass die Werte seltener genannter Anbieter in der Hochrechnung niedriger ausfallen können als die der explizit häufiger genannten.

[371] In 6 Prozent wurde die Formulierung aus dem Gesetz, nämlich „alle, die geschäftsmäßig TK-Dienste erbringen“, benutzt und in 1 Prozent wurde auf „die jeweils zuständigen Netzbetreiber“ verwiesen.

Bei Beschlüssen, die mehrere Anschlüsse betreffen, ist unsicher, ob alle Anschlüsse die genannten Unternehmen verpflichten und ob die genannten Abfragearten alle Anschlüsse bzw. Anbieter betreffen. Dies führt dazu, dass die Hochrechnungswerte umso höher ausfallen können, je differenzierter die Angaben sind, von denen ausgegangen wird. Dabei dürften aber je nach Abfrageart unterschiedliche Fehler auftreten. Insgesamt gesehen stellt aber der gemittelte Wert der Hochrechnungen eine realistische Schätzung dar.

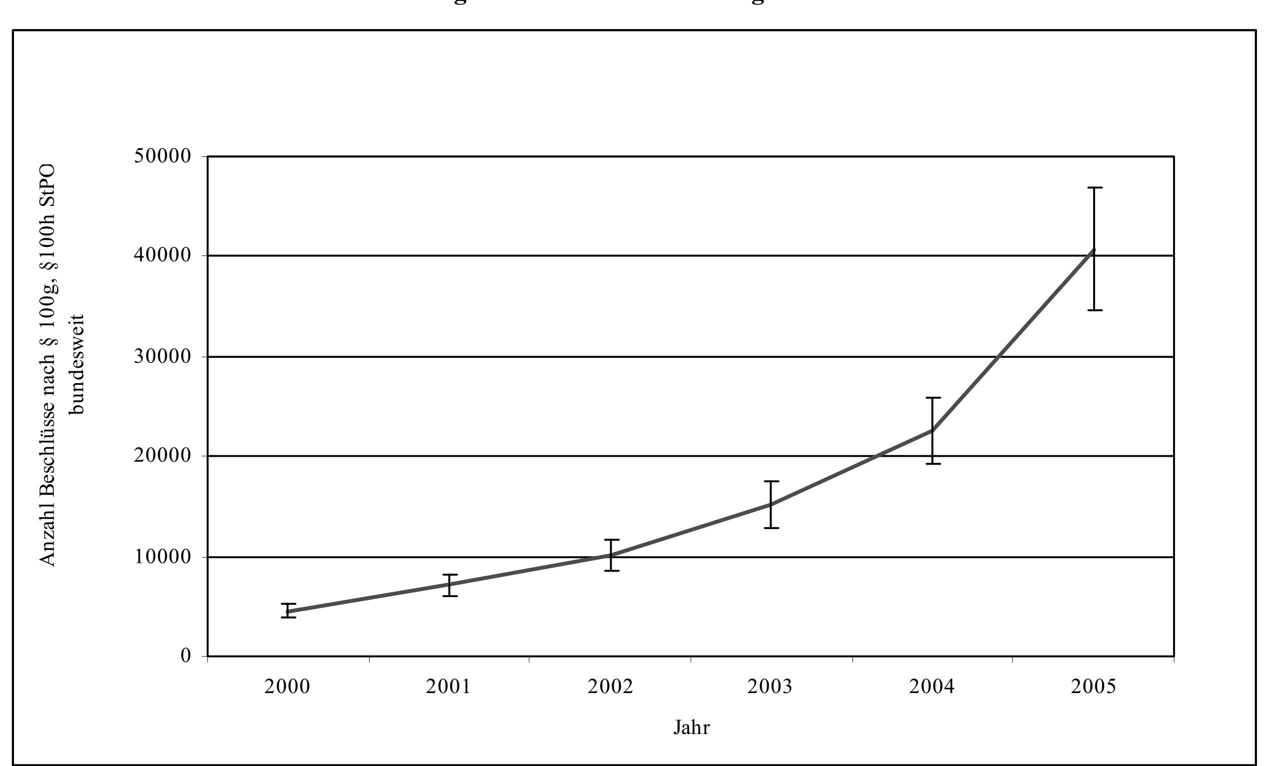
Der in der Abbildung enthaltene mittlere Wert der Hochrechnungen repräsentiert die bestmögliche Schätzung der Anzahl der Beschlüsse nach §§ 100g, 100h StPO. Er ist zusammen mit der Fehlerspanne dargestellt. Danach lag die Zahl der Verkehrsdatenabfragen im Jahr 2005 bei etwa 40 000 (ohne Abfrage der Zuordnung von dynamischen IP-Adressen zu einem Anschlussinhaber bzw. Internetnutzer). Die Tendenz ist stark ansteigend.

2005 wurden demnach erstmals etwa gleich häufig die Abfrage von Verkehrsdaten und Inhaltsüberwachungen angeordnet (Telekommunikationsüberwachung ca. 42 500 Beschlüsse incl. Verlängerungen und ca. 40 000 Beschlüsse zu Verkehrsdatenabfragen). In den Jahren davor lag die Abfrage von Verkehrsdaten noch deutlich unter der Anzahl von Inhaltsüberwachungen (2004: Telekommunikationsüberwachung 34 400, Verkehrsdaten 22 600; 2003: Telekommunikationsüberwachung 29 430, Verkehrsdaten 15 200 und 2002: Telekommunikationsüberwachung 26 200, Verkehrsdaten 10 200).

Abbildung 4



Entwicklung der Verkehrsdatenabfragen 2000 bis 2005



Für die Entwicklung der verschiedenen Arten der Verkehrsdatenüberwachung kann auf detaillierte Angaben einzelner Telekommunikationsunternehmen zurückgegriffen werden. Wie sich die Zahlen auf die verschiedenen Arten der Verkehrsdatenabfrage verteilen, lässt sich Abbildung 5 entnehmen. Die Zahl der Beschlüsse, die eine Abfrage zu einer IMEI-Nummer (International Mobile Equipment Identity) beinhalteten, stieg etwa um das Vierfache. Die angeordneten Zielwahlsuchen, die auch als Zielsuchläufe bezeichnet werden, verdreifachten sich.

Dem entspricht auch das Bild der Entwicklung der Anordnungen nach §§ 100g, 100h StPO im Festnetzbereich. Hier ist ein kontinuierlicher Anstieg der Zielwahlsuchen zu bemerken, während die Abfrage von abgehenden und zukünftigen Verkehrsdaten seit 2003 auf gleichem Niveau bleibt. Ein extremer Anstieg fällt bei der Abfrage von IP-Adressen im Vergleich von 2004 und 2005 auf. Während 2004 noch Daten zu etwa 6 300 IP-Adressen abgefragt wurden, stiegen diese Anordnungen 2005 auf 75 500. Dies hängt mit großflächigen Ermittlungen (insbesondere bei Urheberrechtsverletzungen) zusammen, die 2005 aus den unter Einsatz der Suchsoftware „Logistep“ erzeugten Hinweisen auf IP-Adressen (in P2P-Netzwerken/Tauschbörsen) folgten. Allein im Bereich der Staatsanwaltschaft Karlsruhe gingen 2005 etwa 20 000 Anzeigen (unter Mitteilung von IP-Adressen, Einwahl-Zeitpunkt und Download-Aktivität) von Urheberrechtsverletzungen ein (diese betrafen im Wesentlichen das Spiel „Earth 2160“), die jeweils die Bestimmung der Anschlussinhaber über die Zugangsprovider zur Konsequenz hatten.[372] Im Zusammenhang mit einer längerfristigen Speicherung von Verkehrsdaten wird insoweit der Zugriff im Rahmen des in § 101 (Urheberrechtsgesetz) des Entwurfs eines Gesetzes zur Verbesserung des Schutzes des geistigen Eigentums (Bundestagsdrucksache 16/5939, 4. Juli 2007) verankerten Auskunftsanspruchs gegen Internetzugangsanbieter jedenfalls eine Option bleiben, die sich auf die künftige Struktur und Häufigkeit des Zugriffs auf Bestands- und Verkehrsdaten erheblich auswirken kann. Zudem dürften jedenfalls schwere Verletzungen von Urheberrechten, die über das Internet vollzogen werden, die strafprozessualen Bedingungen des Zugriffs auf gespeicherte Verkehrsdaten erfüllen. Gerade hier zeigt sich im Übrigen das Problem identifizierender Bestandsdaten, die in einer zukünftigen Welt des „Perveasive und Ubiquitious Computing“ eine Schlüsselrolle einnehmen werden.[373]

[372] www.heise.de/newsticker/meldung/67389.
[373] *Roßnagel/Pfitzmann/Garstka*, 2001; *Bizer, u. a.,* 2006.

Abbildung 5

Entwicklung der Verkehrsdatenabfrage im Mobilfunkbereich
(1 Unternehmen, 31,6 Millionen Kunden)

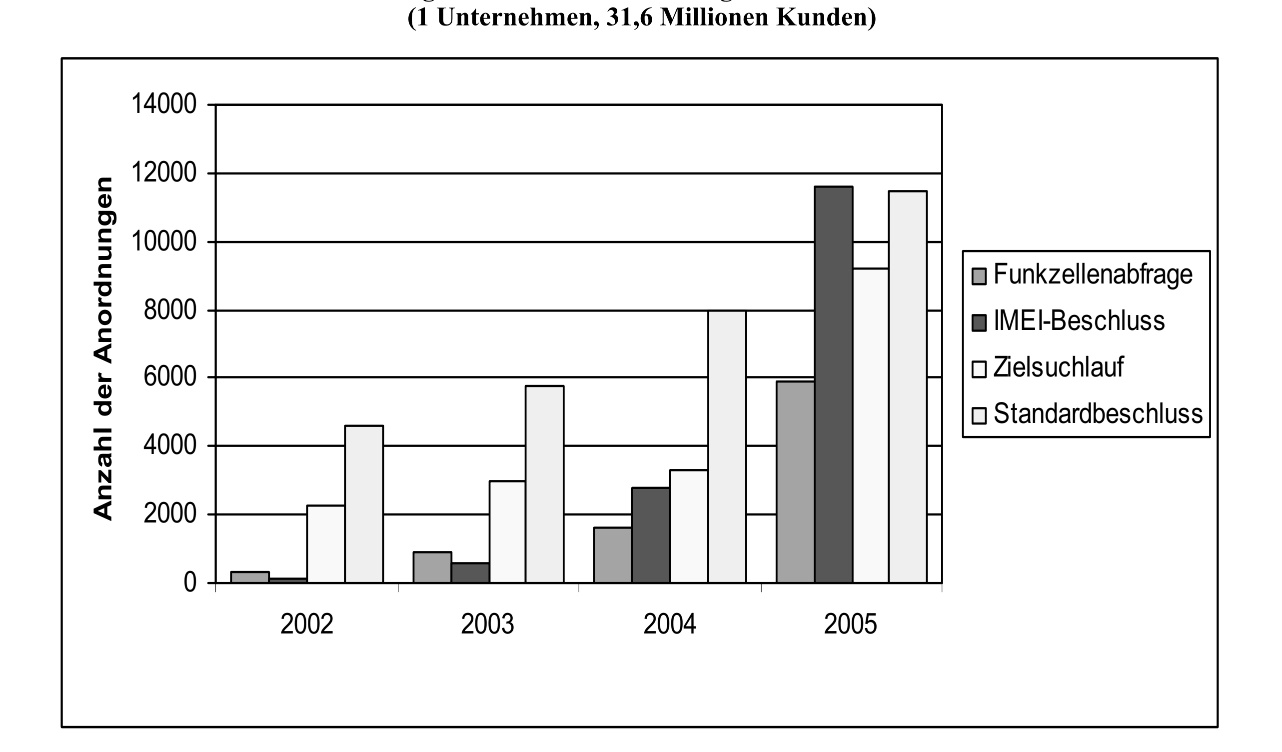
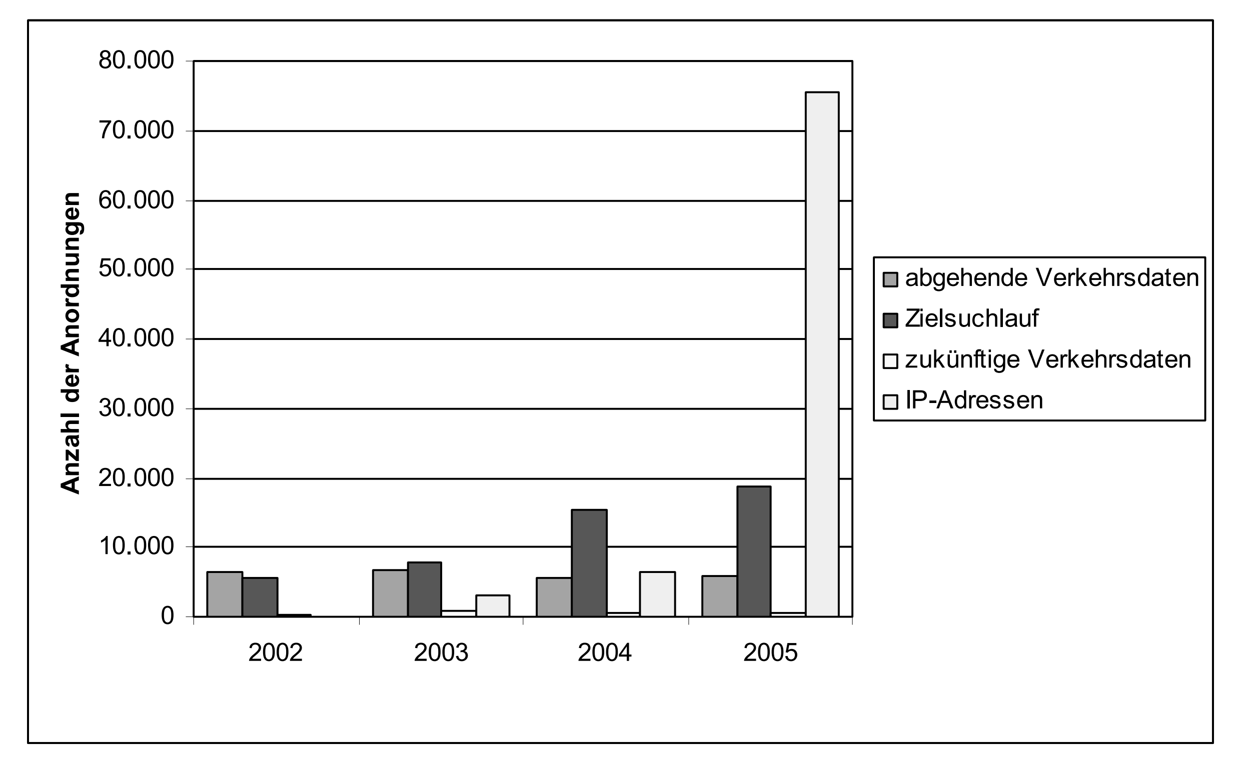


Abbildung 6



Entwicklung der Verkehrsdatenabfrage und der Zuordnung von Nutzern zu dynamischen IP-Adressen im Festnetzbereich (1 Unternehmen, ca. 33 Millionen Anschlüsse)



IV. Empirische Untersuchungen zur Verkehrsdatenabfrage

1. Untersuchungen zu Häufigkeit, Anwendungsstrukturen und Nutzen für die Strafverfolgung

Repräsentative wissenschaftliche Studien zum Gebrauch und zu den Folgen der Abfrage von Telekommunikationsverkehrsdaten liegen in Deutschland bislang nicht vor.[374] Dies gilt freilich auch für andere Länder der Europäischen Union sowie drüber hinaus und ist angesichts der sicherheitspolitischen Einschätzungen der Bedeutung des Zugangs zu Telekommunikationsdaten für Strafverfolgungsbehörden wie für Geheimdienste erstaunlich.[375] Unklarheit herrscht nicht nur über Art, Umstände und Ergebnisse der Abfragen und Auskünfte über Telekommunikationsverkehrsdaten, sondern auch über ihre quantitative Bedeutung. Zwar hat das Bundeskriminalamt, Fachbereich RETASAST, bereits im November 2003 eine interne Erhebung zu Verfahren mit Maßnahmen nach §§ 100g, 100h StPO durchgeführt. Analysiert wurden Verfahren aus dem Bundesland Schleswig-Holstein und solche, die unter Mitwirkung des Bundesgrenzschutzes und des Bundeskriminalamtes stattfanden. Dabei wurde ein Fragebogen entwickelt und für Ermittlungsverfahren des Bundesgrenzschutzes, des Bundeskriminalamtes und des Landes Schleswig-Holstein ausgefüllt. Die Erhebung begann im April 2002 und endete im September 2003. In den erfassten 145 Ermittlungsverfahren wurden nach dieser Studie insgesamt 864 Anträge gemäß §§ 100g, 100h StPO gestellt. Mangels Repräsentativität der Untersuchung können die Ergebnisse allerdings nicht auf das Bundesgebiet übertragen werden.

In der Studie des Max-Planck-Instituts Freiburg zur Telekommunikationsüberwachung nach §§ 100a und 100b StPO[376] wurden auch Abfragen nach dem FAG erfasst. Die Befunde weisen eine erhebliche Anzahl von Fällen aus, in denen es neben Maßnahmen gemäß §§ 100a, 100b StPO auch bzw. ausschließlich zu solchen gemäß § 12 FAG gekommen war. Etwa ein Viertel der Anordnungen enthielt neben der Auskunftsersuchen nach § 12 FAG. Die reinen FAG-Fälle machten 12 Prozent der Beschlüsse bzw. 14 Prozent der Anschlüsse aus.[377] Auch diese Befunde sind für die vorliegenden Fragestellungen nur von begrenztem Aussagewert, denn die Stichprobenziehung der Untersuchung war bedingt durch das Vorliegen der Anordnung einer Telekommunikationsüberwachung gemäß § 100a StPO. Deshalb sind Aussagen über die Verbreitung der Abfragen nach dem FAG nur begrenzt möglich. Für die Abfragen nach dem FAG, die neben Maßnahmen nach §§ 100a, 100b StPO durchgeführt worden sind, wird berichtet, dass diese etwa zu gleichen Teilen auf die Vergangenheit und auf die

[374] Vgl. hierzu zusammenfassend *Albrecht,* 2005; *Breyer,* 2005.
[375] *All Party Parliamentary Internet Group*, 2003, S. 4.
[376] *Albrecht/Dorsch/Krüpe*, 2003.
[377] *Albrecht/Dorsch/Krüpe*, 2003, S. 147.

Zukunft ausgerichtet sind, wobei die Abfragezeiträume weit gefasst waren Die Abfragezeiträume waren aber zum Teil nicht konkretisiert und bezogen sich auf „alle noch verfügbaren Daten", was bedingt sein mag durch die Einschätzung, dass Löschungen die Abfragemöglichkeiten von vorneherein begrenzen. Offensichtlich wird der FAG-Abfrage überwiegend kein eigenständiges Ermittlungsziel zugeordnet.[378] Jedenfalls waren in fast zwei Dritteln der Verfahren Abfragen nach FAG keine Zielsetzungen in den Akten dokumentiert (außerhalb der Zwecksetzungen für die Maßnahmen nach §§ 100a, 100b StPO). Soweit Ziele genannt wurden, waren dies die Feststellung von weiteren Anschlüssen eines Beschuldigten, die Anschlüsse noch nicht identifizierter weiterer Personen sowie die Aufenthaltsbestimmung zu einem bestimmten Zeitpunkt. Für etwa ein Drittel der Abfragen war dokumentiert, dass die Verkehrsdaten übermittelt worden waren. Im Übrigen erklärt die Löschung von Daten teilweise, dass Abfragen nicht umgesetzt werden konnten.[379] Für Anschlüsse, die ausschließlich Abfragen nach FAG unterlagen, wurden folgende Feststellungen getroffen. Der längste abgefragte Zeitraum betrug ein halbes Jahr. Zielsetzungen waren für selbständige FAG Abfragen bei etwa einem Drittel der Fälle nicht in den Akten dokumentiert. Wo Zielsetzungen ausgewiesen waren, handelte es sich um die Feststellung weiterer Anschlüsse des Beschuldigten oder um die Identifizierung von Gesprächspartnern; insoweit geht es um eine typische Konsequenz aus einer Telekommunikationsüberwachung gemäß §§ 100a, 100b StPO. Begründungen der FAG Anordnung finden sich selten; wenn begründet wird, dann durch den Bezug auf Katalogdelikte oder die Subsidiaritätsformel des § 100a StPO.

Die Erkenntnisse aus der Studie von *Backes/Gusy*[380] zu § 12 FAG können deshalb für Aussagen über Anwendungsstrukturen der Verkehrsdatenabfrage nicht genutzt werden, weil in dieser Untersuchung die Abfragen von Verkehrsdaten nur an solchen Stellen in die Auswertung einbezogen worden sind, wo dies sinnvoll erschien.[381] Die Einbeziehung ergab sich offenbar daraus, dass die Abfrage in einzelnen Fällen von den Strafverfolgungsbehörden als Telekommunikationsüberwachung eingestuft wurde.[382]

Kinzig hat in einer Untersuchung zur rechtlichen Bewältigung von Erscheinungsformen organisierter Kriminalität den Einsatz verdeckter Ermittlungsmethoden in solchen Ermittlungsverfahren thematisiert, die von den Strafverfolgungsbehörden organisierter Kriminalität zugeschlagen werden. Damit handelt es sich zwar um eine hoch selektierte Gruppe, freilich um eine solche, auf die die Instrumente verdeckter Ermittlungsmaßnahmen konzentriert sein sollten. Die Ergebnisse der Untersuchungen verweisen einmal darauf, dass der Abfrage von Verkehrsdaten in Verfahren der organisierten Kriminalität ein breiter Anwendungsspielraum zukommt. Verkehrsdaten werden in etwa 40 Prozent der Fälle erhoben. Der Verfasser schließt aus den Daten auch, dass von der Maßnahme weitaus zurückhaltender als von der Telekommunikationsüberwachung Gebrauch gemacht werde.[383]

Eine weitere Untersuchung des Bundeskriminalamts zur Verkehrsdatenspeicherung wurde Ende 2005 mit vorläufigen Ergebnissen veröffentlicht.[384] Die Untersuchung erfasst einen Zeitraum des Jahres 2005 und basiert auf der Verteilung von Fragebögen an Polizeidienststellen der Länder. Unklar ist auf der Grundlage der bisherigen Veröffentlichungen, um welchen Typ von Auswahl bzw. Stichprobenziehung es sich hierbei handelt. Jedenfalls wurden bis zwischen April und November 2005 381 Fälle (Verfahren) gemeldet, in denen Bestands- und/oder Verkehrsdaten abgefragt wurden. Zu den Verfahren wurden Einschätzungen von am Verfahren Beteiligten erhoben, die sich auch auf die Frage bezogen, welche Zeitspanne für eine Verkehrsdatenspeicherung als angemessen angesehen wird. Die gemeldeten Verfahren berühren alle Straftatentypen, lassen allerdings einen Schwerpunkt im Bereich der Sexualdelikte (und Betrugsdelikte) erkennen. Ein Schwerpunkt lag ferner bei Internetverbindungsdaten (ca. 44 Prozent der Fälle), was die Vermutung aufkommen lässt, dass Kinderpornografieverfahren besonders stark vertreten waren. Ebenso häufig bezogen sich die Verfahren auf Telefonkommunikation, der Rest betraf Kombinationen. Der Schwerpunkt lag auf Verkehrsdaten; Bestandsdaten spielten bei etwa einem Fünftel der Verfahren eine Rolle. Die Abfrage scheint in der Mehrzahl der Fälle in das Leere zu laufen, da für etwa 70 Prozent der Fälle angegeben wurde, dass die Betreiberfirmen der Abfrage nicht nachgekommen seien (überwiegend deshalb, weil die entsprechenden Daten gar nicht gespeichert (Flatrate, Prepaid) oder bereits vernichtet waren). Das sog. „Quick Freeze" Verfahren wird von Strafverfolgungspraktikern überwiegend nicht als gleich effiziente Maßnahme beurteilt. Schließlich wird mehrheitlich für eine Speicherungsfrist für Verkehrsdaten von sechs Monaten votiert, wobei sich für Betäubungsmittelverfahren (wohl deshalb, weil hier langfristige Ermittlungen in Netzwerken von Händlern im Vordergrund stehen) eine Präferenz von zwölf Monaten ergibt.

Eine Studie zu den Folgen der Verkehrsdatenabfrage für die Durchführung strafprozessualer Ermittlungen wurde im Jahr 2005 von der Erasmus-Universität (Rotterdam) vorgelegt.[385] Die Untersuchung spielte in den Debatten über die EG-Richtlinie 2006/24 zur Verkehrsdatenerfassung und -speicherung auch deshalb eine herausragende Rolle[386], weil es sich bis dahin um die europaweit einzige empirische Untersuchung zu Verkehrsdaten handelte. Die Untersuchung beruhte auf der Analyse von 65 Strafverfahren, die freilich nicht repräsentativ sind für Strafverfahren insgesamt, oder für Strafverfahren, in denen eine Verkehrsdatenabfrage erfolgte. Vielmehr handelte es sich um vom niederländischen Justizministerium ausgewählte

[378] *Albrecht/Dorsch/Krüpe*, 2003, S. 186 f.
[379] *Albrecht/Dorsch/Krüpe*, 2003, S. 186.
[380] *Backes/Gusy*, 2003.
[381] *Backes/Gusy*, 2003, S. 19.
[382] *Albrecht/Dorsch/Krüpe*, 2003, S. 145; *Backes/Gusy*, 2003, S. 18.
[383] *Kinzig*, 2004, S. 467, unter Berufung vor allem auf durchschnittlich weit geringere Anzahl ausgewerteter Anschlüsse im Fall von FAG-Beschlüssen.
[384] *Mahnken*, 2005.
[385] *Faculteit der Rechtsgeleerdheid, Erasmus Universiteit Rotterdam*, 2005.
[386] *Commission Staff Working Document*, Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, {COM(2005) 438 final}, Brüssel, 21. September 2005, S. 4.

Strafverfahren, von denen angenommen wurde, dass die Verkehrsdatenabfrage nachhaltig zum Erfolg der Ermittlungen beigetragen habe. Die Befunde aus der Aktenanalyse verweisen darauf, dass in allen Verfahren auf die Verkehrsdaten zurückgegriffen werden konnte, die von den Strafverfolgungsbehörden abgefragt wurden.[387] Die Art der Daten, die heute von den Telekommunikationsanbietern für eigene Zwecke gespeichert wird, scheint nach den Untersuchungsergebnissen auch für Zwecke der Strafverfolgung ausreichend zu sein. Die Interpretation der Daten verweist darauf, dass zwei Drittel der Fälle auch ohne die Abfrage der Verkehrsdaten hätten aufgeklärt werden können. Die Daten werden wohl dazu genutzt, die Kommunikationsmuster und Kontaktpersonen abzuklären und die Überwachung von Tatverdächtigen zu unterstützen. Selten kommt es nach dem Bericht dazu, dass Verkehrsdaten, die älter als sechs Monate sind, benötigt werden. Jedoch ergeben sich aus im Rahmen der Studie auch durchgeführten Interviews mit Praktikern aus der Strafverfolgung und der Strafjustiz überwiegend Forderungen nach einer Speicherungsdauer von zwölf Monaten.

In einer vergleichenden Untersuchung zu Systemen der Überwachung von Telekommunikationsverbindungsdaten aus dem Jahre 2004 wurden (unsystematische) Beobachtungen aus den in den Vergleich einbezogenen Ländern zusammengestellt. Die mitgeteilten Befunde beziehen sich zum größeren Teil auf (nicht vollständig nachvollziehbare) Erfahrungsberichte aus unterschiedlichen Bereichen (Politik, Telekommunikationsindustrie, Strafverfolgung). Zunächst wird dort festgehalten, dass keine systematischen Studien zur Wirksamkeit von Vorratsdatenspeicherung hätten identifiziert werden können.[388] Mit Verweis auf Analysen schwedischer Telekommunikationsanbieter wird hervorgehoben, dass die Abfragen der Strafverfolgungseinrichtungen sich auf einen Zeitraum von drei Monaten konzentrierten (85 Prozent der abgefragten Verkehrsdaten sollen sich in Schweden auf einen Zeitraum beziehen, der nicht länger als drei Monate zurückliegt; 10 Prozent auf einen Zeitraum von einem halben Jahr). Für England/Wales wird ebenfalls mitgeteilt, dass sich Abfragen ganz überwiegend (80 Prozent) auf Daten aus den letzten drei Monaten beziehen.[389] Der Bedarf zur Einführung einer Vorratsdatenspeicherung wird auf der Grundlage der beobachteten Praktiken bezweifelt.

Eine Untersuchung zur Rechtslage und zu den Praktiken der Verkehrsdatenspeicherung und -abfrage, die 2006 erschien und sich auf Österreich konzentriert, beruht weitgehend auf Interviews mit wenigen Schlüsselpersonen.[390] Hieraus ergeben sich Feststellungen, die sich im Wesentlichen mit den bereits vorgetragenen Befunden decken. So wird für Österreich mitgeteilt, dass sich die Abfrage von Verkehrsdaten ganz überwiegend auf die letzten drei Monate vor dem Abfragebeschluss beschränke.[391]

[387] *Faculteit der Rechtsgeleerdheid, Erasmus Universiteit Rotterdam*, 2005, S. 38–40.
[388] So auch *Breyer,* 2005.
[389] *Büllingen u. a.,* 2004, S. 8.
[390] *Larnhof*, 2006.
[391] *Larnhof*, 2006, S. 22.

Aus einer schriftlichen Befragung der Mitgliedsländer durch die Europäische Kommission zur Speicherung von Verkehrsdaten ergeben sich Hinweise auf Mitteilungen von Strafverfolgungsbehörden zu wegen fehlender Gesetzgebung zur Datenspeicherungspflicht entstehenden Problemen für Ermittlungen in Strafsachen.[392] Belgien berichtet (wie auch Deutschland, England, Spanien und Portugal) von allgemeinen Klagen der Polizei wegen bereits gelöschter Daten, von Ermittlungsproblemen in größeren Firmen, die Zugang zu Internetdiensten erlauben, und von Verlagerungen der Telekommunikationsunternehmen in Länder mit weniger strikten Regeln. Aus Finnland werden gelegentliche Probleme wegen gelöschter Daten mitgeteilt. Größere Probleme werden freilich in der internationalen Kooperation (auch der europäischen) gesehen. In Frankreich wird davon ausgegangen, dass durch die Gesetzgebung von 2001 (Loi N°2001-1062, „Sicherheit im Alltag“) ein praktikables Instrument geschaffen worden sei. In den Berichten Österreichs, Irlands, Luxemburgs, Schwedens und Griechenlands werden Probleme nicht erwähnt.

Im Übrigen beschränken sich Analysen der Verkehrsdatenabfrage auf die Untersuchung von Einzelfällen und eine eher qualitativ ausgerichtete Folgenabschätzung der Speicherung und Nutzung von Verkehrsdaten für Zwecke der Strafverfolgung. Nicht nur die in zahlreichen Ländern der Europäischen Union geführten Debatten über die Legitimität (und Grundrechtskonformität) der Umsetzung der Europäischen Richtlinie verweisen auf die Nutzung der Einzelfallanalyse, sondern auch die von der Europäischen Kommission selbst vorgelegte „erweiterte“ Folgeneinschätzung (Extended Impact Assessment)[393] bedient sich einer (unsystematischen) Analyse von Einzelfällen, die aus den Mitgliedsländern stammen. Besondere Bedeutung wird in diesem Zusammenhang der Aufklärung von terroristischen Anschlägen wie dem Madrider Anschlag von 2004 (ferner den Anschlägen vom 11. September und dem Omagh Bombenanschlag) zugewiesen.[394] Verschiedene Mordfälle (Frankreich: Mord an Präfekt Erignac, Irland: Mord an der Journalistin Guerin) dienen ebenfalls zur Untermauerung der Annahme, dass Verkehrsdaten für die Aufklärung vor allem schwerer Kriminalität von entscheidender Bedeutung sein können.[395] Er-

[392] *Council of the European Union*, Note, from: General Secretariat to: Multidisciplinary Group on Organised Crime (MDG). Subject: Answers to questionnaire on traffic data retention Brüssel, 14107/02, vom 20. November 2002.
[393] *Commission Staff Working Document*, Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, {COM(2005) 438 final}, Brüssel, 21. September 2005.
[394] So zum Beispiel in der Begründung der französischen Gesetzgebung zur Verkehrsdatenspeicherung, www.senat.fr/ue/pac/E2616.html; vgl. hierzu freilich auch *Schulzki-Haddouti,* 2003, S. 15, mit der Feststellung, dass das Internet in der Vorbereitung der Anschläge vom 11. September keine Rolle spielte.
[395] *Commission Staff Working Document*, Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, {COM(2005) 438 final}, Brüssel, 21. September 2005, S. 3 f.

folgversprechende Ermittlungsansätze werden dann mit dem (aus persönlichen Erfahrungen herrührenden) Befund konfrontiert, dass 30 bis 40 Prozent der Abfragen allein deshalb erfolglos blieben, weil die entsprechenden Daten bereits gelöscht seien. Diese Informationen fügen sich in die systematisch gewonnenen Daten aus der Studie des Max-Planck-Instituts Freiburg zur Telekommunikationsüberwachung ein.

2. Untersuchungen zu den Kosten der Implementation der Vorratsspeicherung

Umfassende Kosten- oder gar Kosten-Nutzen-Analysen liegen im Zusammenhang mit der Vorratsspeicherung und Abfrage von Verkehrsdaten bislang nicht vor. Die Hinweise auf die mit der Vorratsspeicherung und der Abfragepraxis verbundenen Kosten beruhen auf (interessengeleiteten) Schätzungen, die im Wesentlichen von betroffenen Unternehmen vorgelegt wurden. So teilte AOL mit, dass bei etwa 392 000 000 Nutzungsereignissen und knapp 600 000 000 e-mails pro Tag Anlaufkosten von etwa 40 Millionen US-Dollar und laufende Kosten von etwa 14 Millionen US-Dollar anfallen würden. Die All Party Parliamentary Internet Group des englischen Parlaments schätzte die Gesamtkosten im Jahr 2001 (und unter den Bedingungen von RIPA (Regulation of Investigatory Powers Act) sowie des Anti-Terrorismusgesetzes 2001) für England/Wales auf über 100 Millionen Englische Pfund pro Jahr.[396]

In der Erweiterten Folgenabschätzung der Europäischen Union werden Kostenschätzungen verschiedener Unternehmen und Unternehmensverbände berichtet. ETNO (European Association of Telecommunications Network Operators) hat danach die Kosten für eine Speicherung von zwölf Monaten auf über 150 Millionen Euro für ein großes Netzwerk angegeben (über 100 Millionen Euro für die Speicherung in Form von Software, Server und Datensicherheit sowie mindestens 50 Millionen an laufenden jährlichen Kosten). Ein weiterer, großer Internetserviceprovider (ESP-ISP) wird mit einer Schätzung von 61 Millionen Euro für vier Jahre bei einer Speicherungszeit von zwölf Monaten zitiert.[397] Dagegen wären nach dieser Stellungnahme die Kosten bei einer Speicherungsdauer von drei Monaten zu vernachlässigen (da die entsprechenden Daten schon heute für eine solche Dauer gespeichert bleiben). Die angegebenen Kosten enthalten freilich die für Suchläufe und die Abfragepraxis insgesamt zu erwartenden Kosten nicht. Bei der Speicherung von e-mail headers werden Kosten von etwa 163 Millionen Euro für vier Jahre angegeben. Schätzungen entsprechender erheblicher Kosten können auch dem Alvaro Bericht an das Europäische Parlament entnommen werden.[398] Sehr viel geringere Kosten werden dagegen von der niederländischen KPMG in einer Kostenanalyse für das niederländische Justizministerium für zwei Szenarien (12- und 24-monatige Speicherungsdauer) angegeben.[399] Nach dieser Studie bleiben die Kosten im einstelligen Millionenbereich. Dies deckt sich mit Berichten europäischer Regierungen, die in der Erweiterten Folgenabschätzung wiedergegeben sind.[400]

3. Untersuchungen zum Potential von Telekommunikationsverkehrsdaten für soziale Kontrolle

Die drastischen Veränderungen im Kommunikationsverhalten und der ständig anschwellende Datenstrom aus der Telekommunikation, der Informationen zu Interaktionen, Beziehungen, räumliche Bewegungen etc, mit sich führt, hat in den letzten Jahren zunehmend Interesse an sozialwissenschaftlichen Untersuchungen zu der Frage nach sich gezogen, inwieweit auf der Grundlage von Verkehrsdatensätzen Beziehungsflechte identifiziert und Handlungen vorhergesagt werden können.[401] Sozialwissenschaftliche und wirtschaftliche Interessen kommen partiell zur Deckung mit Interessen von Sicherheitsbehörden an der Aufdeckung von kriminellen Netzwerken, an der Einschätzung von Risiken von Terroranschlägen und ganz allgemein an der Verbrechensprävention.[402] Darüber hinaus geht es um die Zukunft der Überwachung (und des Daten- oder Persönlichkeitsschutzes) in Umgebungen, die immer stärker durch die vernetzte, unmittelbare und intelligente Verarbeitung beständig erzeugter personenbezogener Daten geprägt sind.[403]

In einem vergleichenden Ansatz, der Interviewdaten und einen über neun Monaten für Mobiltelefonverbindungen (einschließlich Ortsdaten) sowie Bluetooth-Verkehrsdaten für eine Gruppe von 98 Personen einschließt, wurde die Frage überprüft, wie gut persönliche Beziehungen (Freundschaften, soziale Netzwerke) und individuelle Zustände (Berufszufriedenheit) aus Verhaltensdaten (Verkehrsdaten) und Selbstberichtsdaten prognostiziert werden können.[404] Die Ergebnisse der Analysen zeigen, dass mit den Verkehrsdaten soziale Netzwerke (und zugrunde liegende Beziehungen) besser identifiziert werden können als durch Befragungsdaten. Etwa 95 Prozent der freundschaftlichen Beziehungen zwischen den Personen der Untersuchungsgruppe lassen sich durch die Verkehrsdaten identifizieren. Ebenso treffsicher erweist sich die Bestimmung anderer Beziehungen und ferner individueller Zustände (in der Untersuchung in Form der Arbeitszufriedenheit überprüft). Hervorgehoben wird auch, dass die technisch (und damit ohne zusätzlichen Aufwand) erzeugten Daten etwa 35 Jahren an (Feld-) Beobachtung entsprechen.[405] Dies lässt nicht nur Schlussfolgerungen zum Potential von Verkehrsdaten für die ökonomisch effiziente und aus Netzwerkperspektiven sichere Überwachung großer Personengruppen zu[406], sondern auch Überlegun-

---

[396] *All Party Parliamentary Internet Group,* 2003, S. 22.

[397] *Commission Staff Working Document*, Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, {COM(2005) 438 final}, Brüssel, 21. September 2005, S. 18.

[398] *Nuno Alvaro,* 2005.

[399] *KPMG Informatie Risk Management,* 2004.

[400] *Commission Staff Working Document*, Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, {COM(2005) 438 final}, Brüssel, 21. September 2005, S. 18 f.

[401] Zur allgemeinen Soziologie mobiler Kommunikation vgl. *Geser,* 2004; zu Anwendungen vgl. *François,* 2007; *Mountain,* 2005; *Laasonen,* 2006.

[402] *Bradbury*, Digital Investigation 2005.

[403] *Bizer, u. a.,* 2006; *Langheinrich,* 2007.

[404] *Eagle/Pentland/Lazer*, 2007.

[405] *Eagle/Pentland/Lazer*, 2007, S. 3.

[406] *Taipale*, New York University Review of Law and Security 2006, S. 1ff.

gen zu einem Vergleich von konventionellen Ermittlungsmaßnahmen wie Vernehmung von Zeugen/Beschuldigten (deren Ergebnisse freilich schon immer als notorisch unzuverlässig betrachtet werden) oder die Observation von Zielpersonen und der Verkehrsdatenabfrage. Die Verkehrsdatenabfrage dürfte danach in einigen Bereichen unter dem Gesichtspunkt der Validität der Daten konkurrenzlos sein. Aus ökonomischen Perspektiven zeigt sich eine Überlegenheit insbesondere für präventive und strategische Anwendungsfelder.

Erhebliches Potential von Verkehrsdaten für die strategische Überwachung wird auch in einer Untersuchung nachgewiesen, die auf die Ökonomie der Überwachung großer Gruppen von Personen ausgerichtet war.[407] Ausgehend von der einfachen Überlegung, dass die Überwachung der Kommunikation einer Person immer Informationen über Dritte generiert, wurde ein E-Mail-Datensatz (ca. 2 300 Personen, Zeitraum etwa drei Jahre) an Hand verschiedener Modelle der Selektion von Zielpersonen auf die Frage hin überprüft, welche und wieviele Personen überwacht werden müssen, um eine maximale und kosten-nutzen-effiziente Überwachungsdichte zu erreichen. Die Untersuchung hat gezeigt, dass die Überwachung einer kleinen Gruppe von Personen alle Beziehungen in einem sozialen Netzwerk erkennen lässt. Die Identifizierung solcher – vor allem aus einer ökonomischen Perspektive interessanter – Zielpersonen kann bereits auf der Grundlage einfacher Informationen aus aggregierten Verkehrsdaten erfolgen. Die Beziehungen in den Netzwerken werden – bei einem bestimmten Algorythmus der Auswahl von Zielpersonen – bereits dann vollständig aufgedeckt, wenn 8 Prozent der Gruppe unter Überwachung stehen. Dies heißt nicht nur, dass Verkehrsdaten ein erhebliches Potential für die Identifizierung sozialer Beziehungen in sich tragen. Verkehrsdaten sind für die Auswahl von Zielpersonen, die mit hoher Kosten-Nutzen-Effizienz Überwachung eines großen Personenkreises zulassen, von entscheidender Bedeutung. Die Untersuchungsergebnisse werden dann genutzt, um die tatsächliche Reichweite der in Telekommunikationsüberwachungsstatistiken von England/Wales mitgeteilten Daten im Hinblick auf dritte Personen abzuschätzen. Im Übrigen wird darauf verwiesen, dass die (auf Kosten und Nutzen bezogenen) Aussagen der Studie für offene, große und sich nicht schützende Netzwerke gelten. Bei kleinen und abgeschotteten Netzwerken, wie sie vor allem in der professionellen oder organisierten Kriminalität vorherrschen, dürfte die Kosten-Nutzen-Effizienz weitaus niedriger liegen.

4. Zusammenfassung

Zusammenfassend können folgende Schlussfolgerungen zu empirischen Befunden zur Überwachung von Telekommunikationsverkehrsdaten gezogen werden:

– Die Forschungslage ist defizitär. Aussagekräftige Daten zur Struktur der Anwendung und zu den Folgen der Abfrage von Bestands- und Verkehrsdaten der Telekommunikation liegen nicht vor.

– Die bisherigen empirischen Studien beruhen auf einer (nicht nachvollziehbaren) Selektion oder auf einer gezielten (und interessengeleiteten) Auswahl bzw. auf einer Stichprobenziehung, die an der Überwachung des Telekommunikationsinhalts anknüpft.

– Weit verbreitet ist im Kontext des Gesetzgebungsprozesses die Einzelfallanalyse, die ausreichende Grundlagen für über den Einzelfall hinausreichende, begründete Entscheidungen allerdings nicht liefern kann.

– Die aus den (hier weit gefassten) empirischen Ansätzen resultierenden Befunde verweisen darauf, dass die Nutzung von Telekommunikationsverkehrsdaten auf kurze Zeiträume konzentriert ist. Dies deckt sich mit den aus Untersuchungen der Telekommunikationsüberwachung vorliegenden Ergebnissen.

– Die quantitative Bedeutung der Verkehrsdatenabfrage ist erheblich und liegt heute dort, wo eine statistische Erfassung durchgeführt wird, deutlich über den Zahlen der Überwachung der Telekommunikationsinhalte.

– In Deutschland kann die Zahl der Verkehrsdatenabfragen im Jahr 2005 – bei deutlich ansteigender Tendenz – auf etwa 40 000 geschätzt werden.

– Ausweislich schriftlicher Befragungen von Regierungen (und anderer Stellen) ergibt sich ein gemischtes Bild. Während aus einigen europäischen Ländern keine Probleme mit der derzeitigen Rechtslage zur Verkehrsdatenspeicherung (Speicherung für Rechnungszwecke und dadurch begrenzte Speicherungsdauer) mitgeteilt werden, verweisen andere Länder auf das Problem von Löschungen und hierdurch vereitelter Ermittlungsmaßnahmen.

– Das Spektrum der Delikte, bei denen in der Praxis die Abfrage von Verkehrsdaten genutzt wird, hängt von der in der jeweiligen Untersuchung verwendeten Auswahl ab.

– Jedenfalls dürfte für die Verkehrsdatenabfrage ein sehr viel weiteres Deliktsfeld in Betracht kommen als für die Überwachung der Inhalte der Telekommunikation.

– Für Deutschland zeigt die Praxis auf der Grundlage des FAG, dass Zielsetzungen bei Abfragen der Verbindungs- oder Bestandsdaten in der Regel nicht dokumentiert werden. Freilich lassen die Daten den Schluss darauf zu, dass Beziehungen zwischen Beschuldigten und dritten Personen bzw. die Identifizierung von Personen und Anschlüssen bekannter Personen im Vordergrund stehen.

– Kostenschätzungen lassen ganz erhebliche Varianz erkennen, die von erheblichen finanziellen Belastungen von Telekommunikationsprovidern bis zu kaum spürbaren Investitionen reicht.

– Offensichtlich wird die Verkehrsdatenabfrage in der Strafverfolgungspraxis und in der Rechtspolitik als eine im Vergleich zur Inhaltsüberwachung weniger stark eingreifende Maßnahme angesehen.

– Verkehrsdaten tragen ein hohes Überwachungspotential in sich. Sie sind – besser als andere Daten – dazu geeignet, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren.

---

[407] *Danezis/Wittneben,* 2006.

3. Methodische Vorgehensweise und Durchführung der Untersuchung

A. Methodenwahl

Zur Beantwortung der Fragen der Untersuchung, die sich auf Anwendungsstrukturen und auf die Folgen der Verkehrsdatenabfrage beziehen, wurden verschiedene Methoden der empirischen Sozialforschung herangezogen.

Die Fragestellungen der Untersuchung lassen sich wie folgt zusammenfassen:

- Antrags- und Anordnungspraxis der Auskunftserteilung,
  - Grunddaten zur Praxis der Anordnungen
    - Anzahl der Betroffenen
    - Anlass und Ergebnisse der Maßnahmen
    - welche Straftaten liegen den Anordnungen zugrunde (insbesondere: sind Kinderpornographie, Organisierte Kriminalität und Rauschgiftdelikte die anlassgebenden Delikte?)
- Nutzung der erteilten Auskünfte
- (Beurteilung der) Effizienz der Verkehrsdatenabfrage (auch in Kombination mit anderen Ermittlungsmaßnahmen)
- Verhältnis der Verkehrsdatenabfrage zu anderen Ermittlungsmethoden
- Berücksichtigung der Anordnungsvoraussetzungen (insbesondere Begründung der Maßnahme)
- Verhältnismäßigkeit und Subsidiarität
- Implementation der Regeln über die Einhaltung der Benachrichtigungs- und Vernichtungspflichten
- Rechtliche und praktische Anwendungsprobleme
- Schwächen und Unklarheiten der Normen der §§ 100g, 100h StPO
- Ablauf der Anforderung von Verkehrsdaten und die Interaktionen zwischen Strafverfolgungsbehörden und Telekommunikationsanbietern
- Auswirkungen der Maßnahmen für die Netzbetreiber wie beispielsweise die bei der Durchführung entstehenden Kosten
- Kosten der Abfrage und Kostenersatz

In einer ersten Phase des Projekts erfolgte eine schriftliche Befragung von Staatsanwälten. Der zweite Teil bezieht sich auf die Analyse von Strafverfahrensakten; das dritte Modul beinhaltet die Durchführung von Expertengesprächen. Die Auswahl der Untersuchungsmethoden beruht auf der Überlegung der wechselseitigen Ergänzung der einzelnen Datenzugänge und dem Ziel der Herstellung eines aus objektiven und subjektiven Informationen bestehenden Gesamtbildes der Verkehrsdatenabfrage, die auf in bürokratischen Verfahren erzeugte Informationen zu Verfahrensabläufen und Verfahrensergebnissen ebenso zurückgreift wie auf Einstellungen und Wahrnehmungen und aus Interviews mit Schlüsselpersonen resultierenden Vertiefungen.

Mit der Verwendung einer Mehrmethodenuntersuchung in Form von Aktenanalyse, Befragung und Interview wird einmal auf die spezifische Mischung von Fragen reagiert, die neben (nur) aus Verfahrensakten entnehmbaren Informationen Beobachtungen und Einschätzungen von Praktikern verlangen. Zum anderen verlangt die Folgenabschätzung, wie weiter oben ausgeführt, eine möglichst umfassende (und unterschiedliche Perspektiven erfassende) Erhebung von Informationen, die als Indikatoren für Folgen der Abfrage von Verkehrsdaten genutzt werden können. Im Zusammenhang mit der Darstellung der Verhältnismäßigkeitsprüfung wurde darauf hingewiesen, dass die Bedingung eines milderen, gleich geeigneten Mittels zur Zielerreichung Indikatoren voraussetzt, die aus der Überprüfung der Effizienz der Maßnahme und der relativen Bedeutung der Verkehrsdatenabfrage im Verhältnis zu anderen Ermittlungsmaßnahmen folgen. Solche Indikatoren können nur aus Strafverfahrensakten, Befragung und Interview gezogen werden, da eine direkte Beobachtung der relativen Bedeutung der Ermittlungsmaßnahme nicht möglich ist. Eine direkte Beobachtung setzt ein kontrolliertes Experiment voraus[408], in dem die Rahmenbedingungen gleich gehalten und lediglich die Interventionen variiert werden.[409] Ein solches kontrolliertes Experiment kann für die Beurteilung der Verkehrsdatenabfrage nicht durchgeführt werden. Die Bildung von Kontrollgruppen, die in anderen Bereichen strafrechtlicher Interventionen (insbesondere strafrechtlicher Sanktionen) einen, wenn auch nicht gleichwertigen, Ersatz für kontrollierte Experimente schafft, ist im Feld der empirischen Strafverfahrensforschung jedenfalls dann nicht möglich, wenn es um verdeckte Ermittlungsmethoden geht. Dies zeigt im Übrigen auch die MPI-Studie zur Telekommunikationsüberwachung, in der der Versuch unternommen wurde, eine Kontrollgruppe von Betäubungsmittelstrafverfahren und anderen Verfahren, die nicht einer Überwachung der Kommunikation ausgesetzt waren, zu bilden.[410] Die durch den Einsatz verdeckter Ermittlungsmethoden erzeugten Kombinationen von Ermittlungsmaßnahmen führen aber zu einer Situation, die vergleichbare Fälle (und damit eine Kontrollgruppe von nicht der verdeckten Ermittlungen ausgesetzten Verfahren) in ausreichendem Umfang nicht mehr entstehen lässt.[411] Es bleibt deshalb allein die Identifizierung geeigneter Indikatoren des Nutzens, die sich aus Dokumentenanalyse, Befragung und Interview ziehen lassen und die aus unterschiedlichen Perspektiven und auf unterschiedliche Dimensionen des Verfahrens bezogen, ferner in der Kombination qualitativer und quantitativer Zugänge vergleichende Beurteilungen der Folgen erlauben.

Die schriftliche Befragung konzentrierte sich deshalb auf Staatsanwälte, da diese sowohl im Ermittlungsverfahren als auch im weiteren Verfahrensverlauf mit der Verkehrs-

---

[408] Zusammenfassend *Ortmann,* 2002.
[409] Vgl. hierzu zusammenfassend *Bremer Institut für Kriminalpolitik,* 2000.
[410] Vgl. hierzu insbesondere *Dorsch,* 2005, S. 271ff.
[411] *Dorsch*, 2005, S. 73.

datenabfrage befasst sind und daher über das gesamte Verfahren abdeckende Erfahrungen verfügen. Einschätzungen und Wahrnehmungen von Staatsanwälten ergänzen die aus einer zeitlich versetzt erfolgten Aktenanalyse gezogenen Informationen. Die Auswertung der Verfahrensakten bietet die Möglichkeit, „harte“ Informationen über die Verkehrsdatenabfrage zu erlangen, die mit Befragung und Interview nicht erfasst werden können.

Die Analyse von Strafverfahrensakten zielt im Rahmen der Studie auf Erkenntnisse über die Antrags- und Anordnungspraxis, die Umsetzung der Auskunftserteilung sowie zur Bedeutung der Verkehrsdaten im weiteren Verfahrensverlauf. Anhand der Akten lassen sich außerdem Informationen über die Beschuldigten, die Betroffenen der Maßnahme, zugrunde liegende Straftaten sowie die Kombination der Verkehrsdatenabfrage mit anderen Ermittlungsmaßnahmen gewinnen. Dabei ist selbstverständlich zu berücksichtigen, dass bestimmte Informationen (z. B. Antworten und Rechnungen der Anbieter) nur teilweise in Akten vorhanden sind.

Die Interviews dienen insoweit vor allem dazu, aus der Perspektive von Experten oder Schlüsselpersonen Erfahrungen und Einstellungen zu erfassen.[412] Die Erkenntnisse aus der Auswertung der Strafverfahrensakten beeinflussten das dritte Modul des Projekts, die Expertengespräche. Anhand der Akten konnten Ergebnisse gewonnen werden, die die Basis für vertiefende Fragen und damit Ansätze zur Interpretation bilden. Durch die Interviews wird eine Vertiefung und Verbreiterung der Interpretation der Ergebnisse der anderen Module ermöglicht. Ferner wird die unterschiedliche Handhabung der Ermittlungsmethode in den verschiedenen Berufsfeldern und Bundesländern erfasst. Dabei geht es auch um Beurteilungen und Sichtweisen verschiedener Berufe und Positionen in Verfahren und im rechtspolitischen Diskurs über die Abfrage von Verkehrsdaten. Deshalb wurden Richter, Staatsanwälte, Polizeibeamte, Verteidiger, Datenschützer und Mitarbeiter von Telekommunikationsunternehmen interviewt.

Im Folgenden werden zunächst die Untersuchungsmodule vorgestellt, die Konzeptionen der Erhebungsinstrumente erörtert und schließlich die Durchführungsmodalitäten beschrieben.

B. Schriftliche Befragung

I. Teilnehmer und Reichweite

Eine bundesweite schriftliche Befragung von Staatsanwälten bildete den ersten Schritt der Untersuchung und zielte auf Erfahrungen mit der Antrags- und Anordnungspraxis bei der Verkehrsdatenabfrage sowie auf Einstellungen zu gesetzlichen Regelungen und ihrer Umsetzung. Die Entscheidung, die Befragung auf die Staatsanwaltschaft zu konzentrieren, ist begründet dadurch, dass deren praktische Erfahrungen das gesamte Verfahren abdecken. Die Staatsanwaltschaft entscheidet im Ermittlungsverfahren darüber, ob eine (von der Polizei angeregte) Maßnahme nach §§ 100g, 100h StPO in Betracht kommt. Wird die Verkehrsdatenabfrage für erforderlich gehalten, so wird entweder ein Antrag beim Gericht auf Erlass eines Beschlusses gestellt oder – bei Gefahr im Verzug – eine Eilanordnung erlassen. Außerdem ist die Staatsanwaltschaft für die Durchführung der Maßnahmen zuständig sowie für die Umsetzung ggf. erforderlicher Folge-Maßnahmen, wie z. B. die Benachrichtigung der Betroffenen. Schließlich erfährt sie durch ihre Stellung als Anklagevertreterin, welche Bedeutung die Daten im weiteren Verfahrensverlauf eingenommen haben. Die Befragung bezog sich auf die Grundgesamtheit der Staatsanwälte.

II. Fragebogenkonzeption

Für die bundesweite schriftliche Befragung von Staatsanwälten wurde ein Fragebogen konzipiert, der sowohl geschlossene Fragen als auch Fragen mit offenen Antworten enthielt und einem Pretest unterzogen wurde. Neben Fragen zur Praxis der Anordnung der Verkehrsdatenabfrage und ihrem Umfang wurden Einstellungen zu den rechtlichen Regelungen und Einschätzungen der Effizienz der Verkehrsdatenabfrage einbezogen. Im Fragebogen wurden die folgenden Themenkomplexe angesprochen:

- Delikte und Verdachtsgrad
- Verhältnis zu anderen Ermittlungsmaßnahmen und speziell zur Telekommunikationsüberwachung
- Antragstellung
- Anordnungen
- Ablehnung von Anträgen und Eilanordnungen
- Dauer der Maßnahmen
- Durchführung der Maßnahmen
- Benachrichtigung der Betroffenen
- Zeugnisverweigerungsrecht
- Kosten und technische Umsetzung
- Probleme der Normanwendung
- Häufigkeit der Maßnahmen
- Erfolgsaussichten
- Zusammenfassende Beurteilungen der Bedeutung der Maßnahmen

III. Durchführung

Nach Fertigstellung wurden die Fragebögen an die Justizministerien der Bundesländer verschickt. Die Fragebögen wurden dann auf dem Dienstweg von den Ministerien an die Generalstaatsanwaltschaften und von diesen an die Staatsanwaltschaften weitergeleitet. Die Anschreiben an die Justizministerien enthielten den Hinweis, dass der

[412] *Mayer*, S. 36.

Fragebogen auch auf den Internetseiten des Max-Planck-Instituts für Strafrecht zur Verfügung stand.

Über die Justizverwaltungen wurden 4 650 Fragebögen an die Staatsanwaltschaften verschickt. Der enge Zeitplan der Untersuchung erlaubte nur ein Erinnerungsschreiben. Jedoch wurden nicht antwortende Staatsanwaltschaften über das Erinnerungsschreiben hinaus noch telefonisch kontaktiert. Die Rücklaufquote beläuft sich auf 19 Prozent. Von 4 650 Fragebögen wurden 874 Fragebögen zurückgeschickt. Freilich dürfte dies im Rahmen der für schriftliche Befragungen erzielbaren Rücklaufquoten liegen. Ausfälle entstanden nicht allein aus Nichtbeantwortung. Zwei Staatsanwaltschaften haben den Fragebogen „als Querschnitt für die gesamte Behörde“ ausgefüllt. Da es bei der schriftlichen Befragung um die subjektive Einschätzung von Individuen geht, konnte eine Beantwortung des Fragebogens für eine ganze Abteilung nicht als solche berücksichtigt werden. Die Erinnerungsschreiben führten dazu, dass etwa 50 weitere Fragebögen eingegangen sind. Dies verweist darauf, dass auch mit weiteren Erinnerungen die Gesamtrücklaufquote nicht hätte wesentlich gesteigert werden können. Staatsanwaltschaften wiesen als Begründung für die Nichtteilnahme auf die hohe Arbeitsbelastung und die daraus resultierende fehlende Zeit zur Beantwortung des Fragebogens hin. Die Fragebögen wurden von studentischen Mitarbeitern elektronisch erfasst.

1. Rücklauf nach Bundesländern

Der Eingang von 874 Fragebögen aus 4 650 verschickten Fragebögen entspricht einer Rücklaufquote von 19 Prozent. Damit liegt der Rücklauf in einem Bereich, der in der sozialwissenschaftlichen Literatur für schriftliche Befragungen angegeben wird. Danach lassen sich in schriftlichen Befragungen Rücklaufquoten zwischen 15 Prozent und 40 Prozent erzielen.[413] Die absolute Zahl der zurückgeschickten Fragebögen wie auch die Rücklaufrate differierten – wie in zu sehen ist – in den Bundesländern.

Ein hoher Anteil der Fragebögen bezieht sich auf das Bundesland Sachsen (219). In diesem Bundesland war auch die Rücklaufrate mit 67 Prozent am höchsten. Die geringste Rücklaufquote war mit 5 Prozent in Berlin festzustellen. In Bremen nahmen fünf Staatsanwälte an der Befragung teil, was einer Rücklaufrate von 13 Prozent entspricht. Aus Baden-Württemberg gingen 121 Fragebögen bei einer Rücklaufquote von 29 Prozent ein. 71 Staatsanwälte aus Mecklenburg-Vorpommern haben den Fragebogen beantwortet, was zu einer Rücklaufquote von 46 Prozent führt. Nordrhein-Westfalen fällt ebenfalls mit einer geringen Rücklaufquote (9 Prozent) auf. Aus diesem Bundesland wurden 82 Fragebögen zurückgeschickt.

[413] *Berekoven/Eckert/Ellenrieder*, 1991, S. 104.

Abbildung 7



Rücklauf und Anzahl differenziert nach Bundesländern

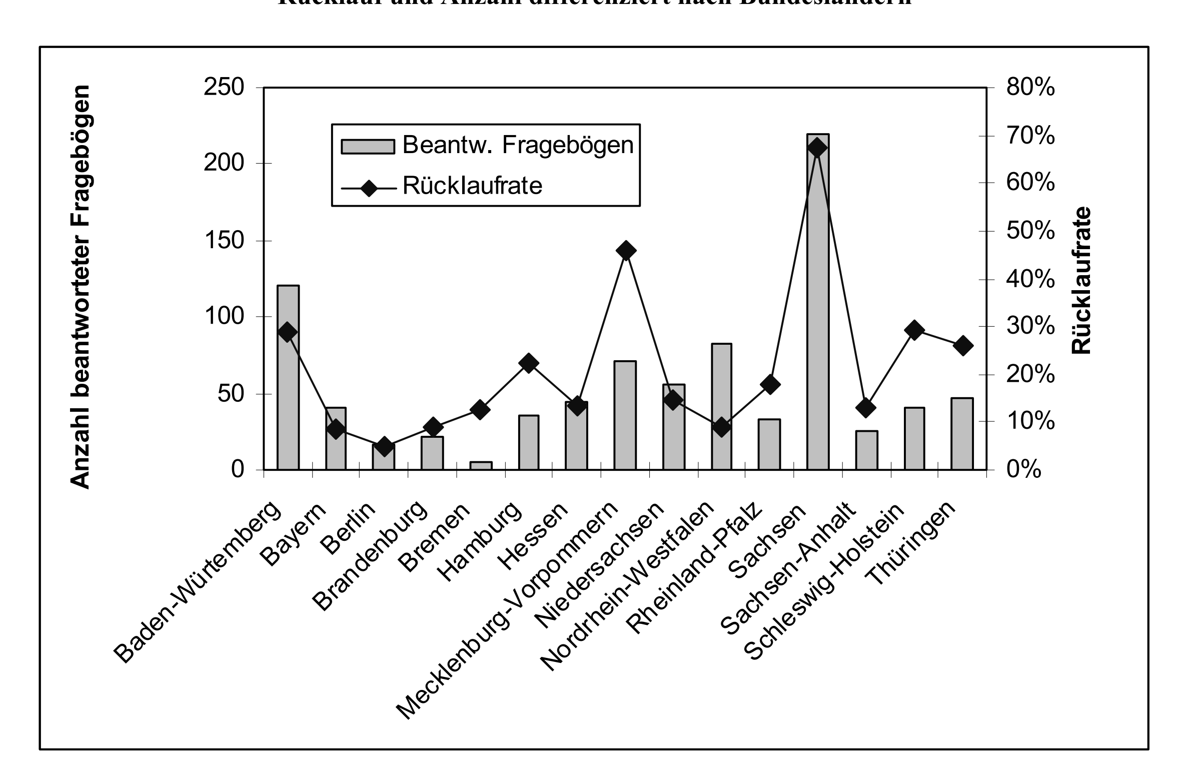


Tabelle 2

Rücklauf in den Landgerichtsbezirken

	Anzahl LG-Bezirke in den Ländern	Antworten aus LG-Bezirken
Baden-Württemberg	17	17
Bayern	22	15
Berlin	1	1
Brandenburg	4	4
Bremen	1	1
Hamburg	1	1
Hessen	9	9
Mecklenburg-Vorpommern	4	4
Niedersachsen	11	11
Nordrhein-Westfalen	19	9
Rheinland-Pfalz	8	7
Saarland	1	0
Sachsen	6	6
Sachsen-Anhalt	4	3
Schleswig-Holstein	4	3
Thüringen	4	4

Die Bundesländer unterscheiden sich zwar in den Rücklaufraten. Jedoch liegen mit der Ausnahme des Saarlands Antworten aus allen Bundesländern vor. Im Übrigen werden in fast allen Bundesländern die Landgerichtsbezirke und damit die Staatsanwaltschaften annähernd komplett abgedeckt. Ferner liegen auch aus den Bundesländern Nordrhein-Westfalen und Bayern Fragebögen aus einer solchen Anzahl von Staatsanwaltschaften vor, die es erlaubt, davon auszugehen, dass die Variationsbreite von Einstellungen und Wahrnehmungen innerhalb der jeweiligen Staatsanwaltschaft im Hinblick auf die Praxis der Verkehrsdatenabfrage abgebildet wird.

2. Rücklauf nach Alter und Geschlecht

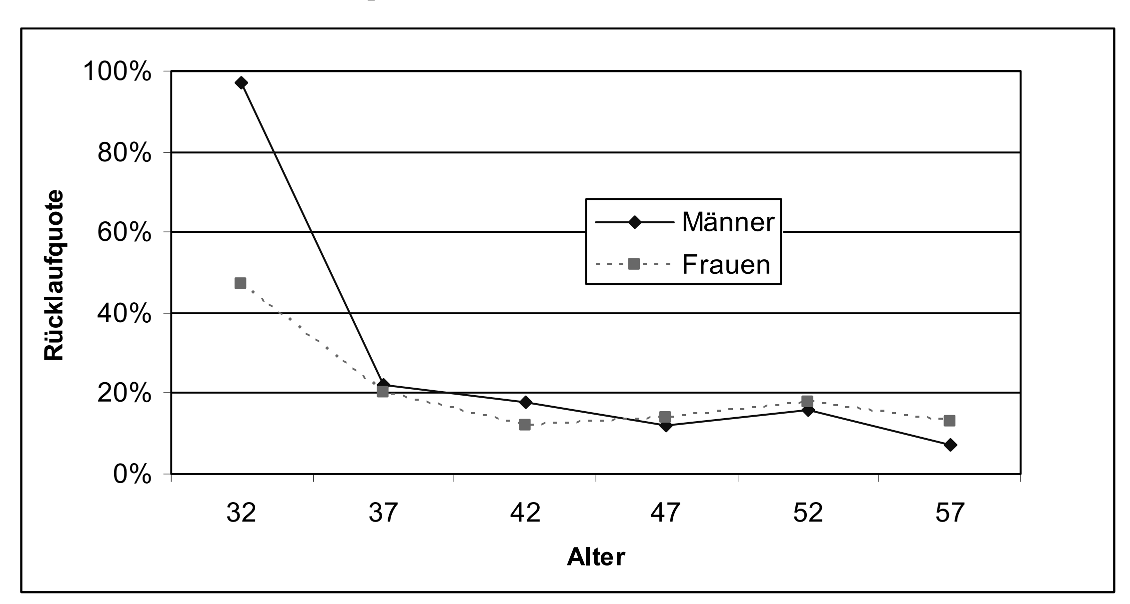
Für die Untergruppe der auch in die Aktenanalyse miteinbezogenen Bundesländer wurde anhand des Handbuchs der Justiz[414] die Alters- und Geschlechtsverteilung in den Staatsanwaltschaften bestimmt. Damit war es möglich für diese vier Bundesländer die Rücklaufraten alters- und geschlechtsspezifisch zu berechnen (siehe Abbildung 8).

Die Rücklaufquote hängt insbesondere vom Alter ab. Auffällig ist, dass in der Gruppe der 30- bis 35-Jährigen eine hohe Rücklaufquote vorliegt, während die älteren Altersgruppen einen geringeren Rücklauf (ca. 15 Prozent) aufweisen. Zwischen den älteren Altersgruppen sind nur geringe Unterschiede festzustellen, wobei die Rücklaufquote mit dem Alter leicht absinkt. Unterschiede in der Rücklaufrate liegen auch zwischen den Geschlechtern vor (Rücklaufquote insg.: Frauen 21 Prozent, Männer 29 Prozent). Die Differenz entsteht fast ausschließlich bei den jüngeren Befragten. Interpretationsmöglichkeiten der Unterschiede liegen unter Umständen in einer häufigeren Teilzeitbeschäftigung gerade jüngerer Frauen in den Staatsanwaltschaften (und damit zusammenhängender Bereitschaft, an der Befragung teilzunehmen). Unterschiede entlang des Alters mögen ggfs. Unterschiede in der Vertrautheit mit moderner Kommunikationstechnologie widerspiegeln.

[414] *Deutscher Richterbund* (Hrsg.), 2004.

Abbildung 8

Rücklaufquote differenziert nach Geschlecht und Alter



3. Alter, Berufserfahrung und Tätigkeitsschwerpunkt der Befragten

Tabelle 3 zeigt, in welchen Dezernaten die Befragten beschäftigt sind. Dabei ist zu beachten, dass etwa ein Viertel der Befragten (27 Prozent der Befragten) angab, in zwei oder mehreren der genannten Dezernate zu arbeiten. Dies führt zu unterschiedlichen Prozentwerten, je nachdem, ob als Bezugsgröße die Anzahl der Nennungen (einschließlich der Mehrfachnennungen) oder die Anzahl der Befragten gewählt wurde. Entsprechend summieren sich die Werte bezogen auf die Befragten auf über 100 Prozent.

Rund 39 Prozent der Befragten arbeiten in einem allgemeinen Dezernat. Etwa 18 Prozent der Staatsanwälte gaben an, dass sie im Bereich der Wirtschaftskriminalität arbeiten, weitere 15 Prozent sind mit der Strafverfolgung von Rauschgiftdelikten und rund 13 Prozent mit Jugendsachen betraut. Ca. 12 Prozent der Befragten arbeiten im Bereich Organisierte Kriminalität. Speziell in der für Verkehrsdatenabfragen besonders interessanten Abteilung Computer- und Internetkriminalität ist ca. 1 Prozent der Befragten beschäftigt. Die Verteilung über Dezernate belegt auch, dass es mit der Befragung gelungen ist, die gesamte Bandbreite staatsanwaltschaftlicher Tätigkeitsfelder abzudecken.

Die Häufigkeit der Nennungen einzelner Dezernate ist in den Bundesländern ähnlich ausgeprägt. Ausnahmen sind Brandenburg mit häufigeren Nennungen der Dezernate organisierte Kriminalität (52 Prozent) und Computer- und Internetkriminalität (14 Prozent), Hessen mit häufigerem Vorkommen von Betäubungsmittel-Dezernaten (31 Prozent), Niedersachsen mit häufigeren Nennungen der Dezernate organisierte Kriminalität (30 Prozent) und Betäubungsmittel (32 Prozent) und Sachsen mit einer unterdurchschnittlichen Anzahl bei Betäubungsmittel-Dezernaten (7 Prozent) und überdurchschnittlichen Werten bei Verkehrsstrafsachen (8 Prozent) und sonstigen Dezernaten (22 Prozent).

Tabelle 3

Dezernate

Dezernat	Anzahl Nennungen	Prozent der Nennungen	Prozent der Befragten (N = 874)
Allgemeines Dezernat	338	*30,9 %*	*39,3 %*
Wirtschaftskriminalität	157	*14,4 %*	*18,2 %*
Betäubungsmittel	130	*11,9 %*	*15,1 %*
Jugendsachen	112	*10,2 %*	*13,0 %*
Organisierte Kriminalität	106	*9,7 %*	*12,3 %*
Sexualdelikte	55	*5,0 %*	*6,4 %*
Kapitaldelikte	40	*3,7 %*	*4,6 %*
Verkehrssachen	22	*2,0 %*	*2,6 %*
Computer- und Internetkriminalität	12	*1,1 %*	*1,4 %*
Sonstiges Dezernat	122	*11,2 %*	*14,2 %*
Insgesamt	**1094**	***100 %***	***127,1 %***

Die Altersverteilung der Befragten entspricht nur bei den über 35-Jährigen der tatsächlichen Verteilung des Alters bei dieser Berufsgruppe, da die unter 35-Jährigen um ca. einen Faktor 3 überrepräsentiert sind (siehe Abbildung 9).

Die Befragten waren durchschnittlich 11,5 Jahre bei der Staatsanwaltschaft tätig (Median zehn Jahre). Es überwiegen Tätigkeitsdauern von bis zu 18 Jahren (siehe Abbildung 10). Eine längere Berufserfahrung weisen 21 Prozent der Befragten auf.

Abbildung 9

Altersverteilung der Befragten

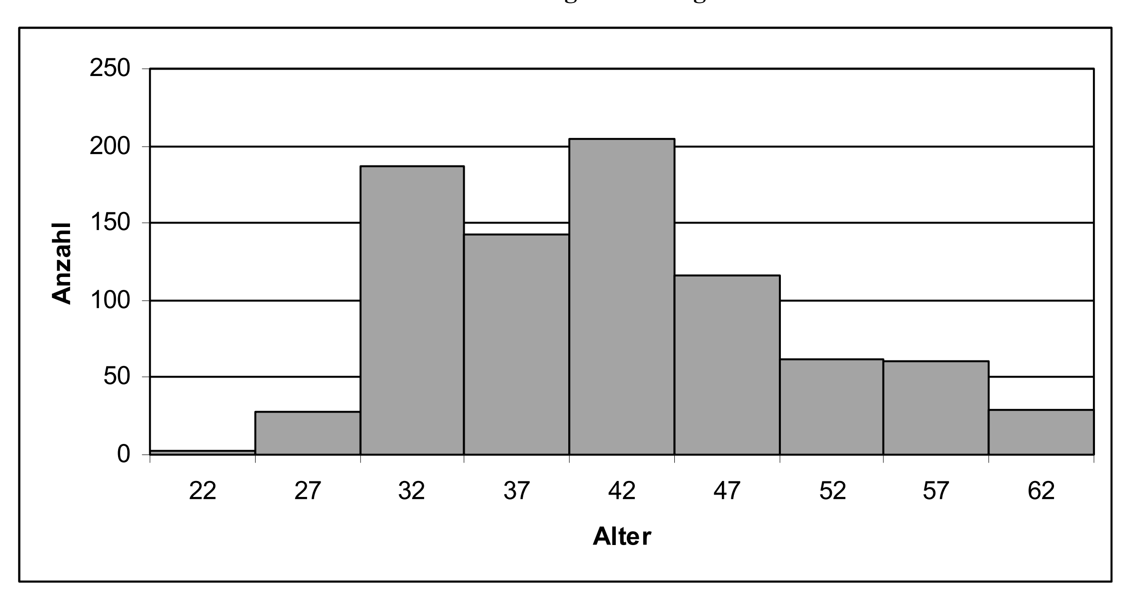
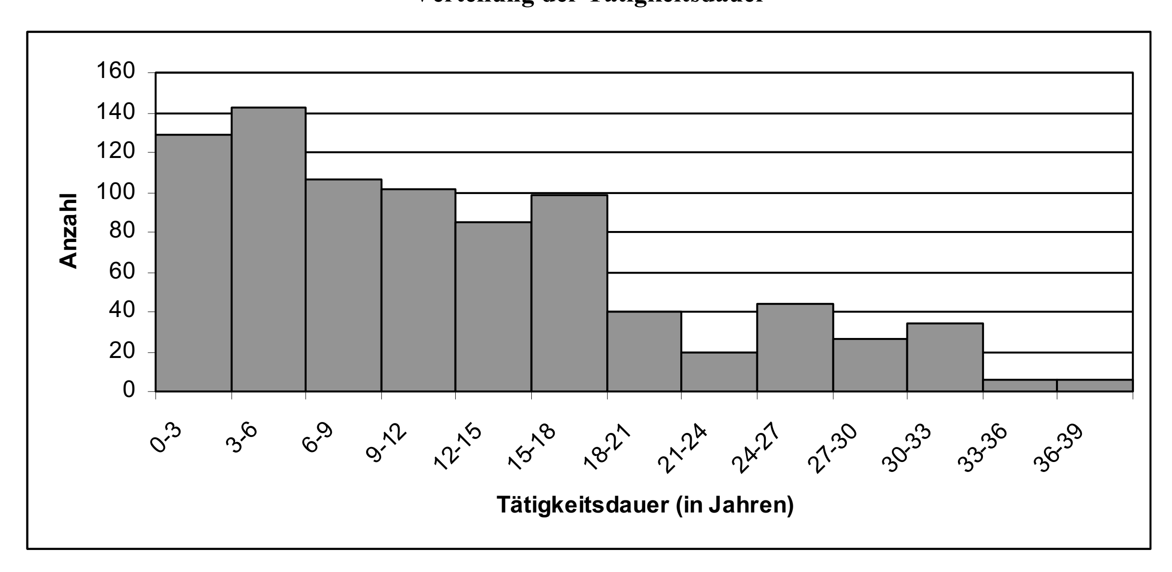


Abbildung 10

Verteilung der Tätigkeitsdauer



Aufgrund von Abteilungswechseln ist die Tätigkeitsdauer in den aktuell genannten Dezernaten mit durchschnittlich 5,4 Jahren geringer als die Gesamttätigkeitsdauer bei der Staatsanwaltschaft. Der wesentlich niedrigere Medianwert[415] von drei Jahren weist darauf hin, dass kürzere Tätigkeitsdauern häufiger auftreten, wobei einzelne Befragte sehr lange Beschäftigungszeiten nennen.

Die Beschäftigungsdauer unterscheidet sich in den verschiedenen Dezernaten nicht in statistisch signifikanter Weise. Gleichwohl ist eine etwas kürzere Beschäftigungsdauer bei Computer- und Internetkriminalität, bei Sexualdelikten und Verkehrsdelikten zu bemerken (< vier Jahren). Längere Beschäftigungszeiten lassen die Dezernate Betäubungsmittel und Kapitaldelikte beobachten (> sechs Jahre). Die durchschnittliche Dezernatsgröße liegt bei sechs Stellen (Mittelwert: sechs, Median: sechs).

Zusammenfassend lässt sich für die schriftliche Befragung feststellen, dass jüngere Altersgruppen überrepräsentiert sind. Die räumliche Verteilung des Rücklaufs deckt – trotz Unterschieden – die Bundesländer und innerhalb der Bundesländer die Landgerichtsbezirke ab. Dasselbe gilt für die verschiedenen Dezernate. Insgesamt ist deshalb von einer Stichprobe auszugehen, die die Variationsbreite von Einstellungen, Perzeptionen und Wissen innerhalb der Staatanwaltschaft erschließen lässt.

C. Aktenanalyse

I. Einführung

Die Aktenanalyse bildet das Kernstück der Studie. Aus den Akten ergeben sich für die Untersuchung zentrale Informationen über die Verfahrensauslösung, die Initiierung, Antragstellung und Anordnung der Verkehrsdatenabfrage, die Begründungen von Polizei, Staatsanwaltschaft und Gericht, die den Anordnungen zugrunde liegenden Delikte und die Bedeutung der Daten sowie etwaige Folgemaßnahmen, Anklage, Hauptverhandlung und Rechtsmittelverfahren. Die Aktenanalyse erstreckte sich dann auf die Durchführung anderer Ermittlungsmaßnahmen, ferner auf Interaktionen zwischen Strafjustiz und Telekommunikationsunternehmen. Die Rechnungen der Telekommunikationsanbieter und die Begleichung der Rechnungen durch die Polizei- und Justizbehörden waren in den Akten teilweise nur unvollständig enthalten. Die Akten waren auch im Übrigen erwartungsgemäß nicht immer vollständig. Zudem bestand ein Teil der Akten aus Verfahren, aus denen andere Verfahren abgetrennt waren oder die zu einem Sammelverfahren gehörten. Auch dies liegt im Rahmen des Erwartbaren. Bei Unvollständigkeit der Akten wurden die Staatsanwaltschaften kontaktiert, um, für die Untersuchung relevante, fehlende Teile anzufordern. In seltenen Fällen war die Vervollständigung wegen Unabkömmlichkeit von Akten nicht möglich.

[415] Median: 50 Prozent der Befragten liegen unterhalb dieses Wertes, die anderen 50 darüber.

II. Stichprobenziehung

1. Vorbereitung

Die Justizbehörden führen keine separate Statistik über die Anordnungen nach §§ 100g, 100h StPO. Die einzige Möglichkeit der Identifikation der einschlägigen Verfahren bestand demnach darin, die bei den Netzbetreibern gespeicherten Daten zu den Anforderungen von Verkehrsdaten heranzuziehen. Die Aktenzeichen wurden aus den §§ 100g, 100h-Beschlüssen bei den führenden Telekommunikationsanbietern Arcor, E-Plus, o2, T-Com, T-Mobile und Vodafone erhoben. Als Konsequenz des Aktenzugangs konnten allerdings nur solche Verfahrensakten angefordert werden, bei denen tatsächlich eine (Eil-) Anordnung nach §§ 100g, 100h StPO ergangen und den Netzbetreibern zugegangen ist. Ablehnungen von Anträgen auf Durchführung von Verkehrsdatenabfragen wurden daher nicht systematisch erfasst.

Die Kooperation mit den Telekommunikationsfirmen verlief ohne Probleme. Nachdem bei den Telekommunikationsanbietern die entsprechenden Daten erhoben worden waren, stand ein umfassender Datenpool zur Verfügung. Die Diensteanbieter übermittelten die Aktenzeichen der Beschlüsse bzw. der Verfahren, das Datum des Beschlusses sowie die Staatsanwaltschaft bzw. das Gericht, welches die Maßnahmen angeordnet hatte. Zum Teil konnte auch nur das Polizeipräsidium, in dessen Bezirk die Anordnung erging, bzw. das Landeskriminalamt des jeweiligen Bundeslandes festgestellt werden. In diesen Fällen wurden die jeweiligen Aktenzeichen einer Staatsanwaltschaft zugeordnet.

Die bei den Anbietern erhobenen Daten umfassten unterschiedliche Aktenzeichen. Zu einem großen Teil waren dies ermittlungsrichterliche Aktenzeichen (Gs-Aktenzeichen), im Übrigen Verfahrensaktenzeichen (Js- und UJs-Aktenzeichen) und zu einem geringen Anteil polizeiliche Vorgangsnummern.

2. Stichprobenziehung und Repräsentativität

Die Aktenanalyse umfasst die Auswertung von Verfahrensakten aus den Jahren 2003 und 2004 aus den Bundesländern Baden-Württemberg, Berlin, Mecklenburg-Vorpommern und Nordrhein-Westfalen. Durch diese Auswahl wurden relevante Unterschiede zwischen den Bundesländern berücksichtigt. Daneben war Mecklenburg-Vorpommern als ein neues Bundesland von besonderem Interesse. Die Erhebungsjahre 2003 und 2004 wurden ausgewählt, da davon ausgegangen wurde, dass die Verfahren aus diesen Jahren einerseits bereits abgeschlossen sind und andererseits nicht zu lange zurückliegen. Nach der Aufnahme der Daten bei den Telekommunikationsanbietern wurden diese nach Bundesländern sortiert und eine Zufallsstichprobe von Aktenzeichen gezogen. In jedem Bundesland sollten 150 Verfahren ausgewertet werden.

Informationen zu den bearbeiteten Beschlüssen konnten fünf Anbieter für den Referenzzeitraum (2003 und 2004) vollständig zur Verfügung stellen. Bei einem Anbieter

waren nur noch die Daten des letzten Quartals von 2003 sowie des Jahres 2004 komplett vorhanden. Dieser Ausfall wie auch die Vernachlässigung der kleineren Telekommunikationsanbieter stellt die Repräsentativität der Basis der Stichprobe nicht in Frage, da sich zum einen Verbindungsdatenabfragen aus technischen Gründen z. B. bei der Zielwahlsuche meist nicht auf einen Anbieter alleine beziehen (die Aktenanalyse ergab, dass im Mittel ca. drei Telekommunikatinsanbieter pro Beschluss abgefragt wurden), zum anderen die auf diese Weise erfassten Beschlüsse wohl über zwei Drittel der insgesamt erlassenen Beschlüsse umfassen. Es gibt keinen Grund anzunehmen, dass die nicht erfassten Beschlüsse Verfahren zuzuordnen wären, die sich durch Besonderheiten auszeichnen.

Zu erwähnen ist in diesem Zusammenhang auch, dass die von den Telekommunikationsanbietern übermittelten Informationen zum Teil nicht beschluss-, sondern anschlussbezogen waren. Die Informationen wurden aber innerhalb der Datensätze der einzelnen Telekommunikationsanbieter beschlussbezogen zusammengefasst soweit das Beschlussdatum, der Sitz der beantragenden Stelle und das jeweilige Aktenzeichen übereinstimmten.

Auf der Basis der von den sechs größten Telekommunikationsanbietern und damit fast aller in den Referenzjahren erlassenen Beschlüsse nach §§ 100g, 100h StPO wurde die Aktenstichprobe bestimmt. Dazu wurden in jedem der vier zu untersuchenden Bundesländer durch Zufall[416] jeweils ca. 180[417] Beschlüsse ausgewählt. Die relativ niedrige Auswahlquote von ca. 2 Prozent (im Fall von Baden-Württemberg und Berlin, sowie 1,1 Prozent in Nordrhein-Westfalen bzw. knapp 9 Prozent in Mecklenburg-Vorpommern) führte dazu, dass in sehr seltenen Fällen ein Beschluss doppelt ausgewählt wurde (<1 Prozent).[418] Auch die Zahl der auf diese Weise doppelt gezogenen Verfahren lag deutlich unter 1 Prozent.[419]

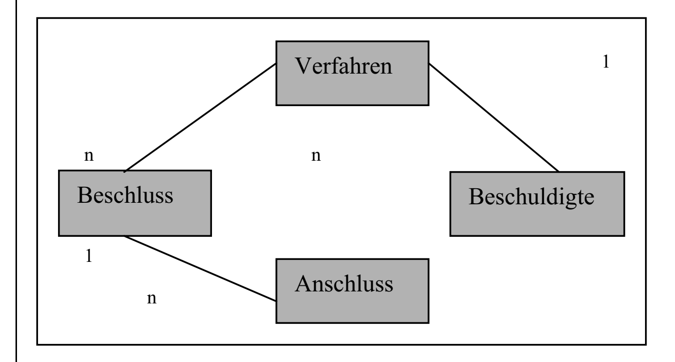
Die so gezogene Stichprobe von Verfahren, in denen nach §§ 100g, 100h StPO Verkehrsdaten abgefragt wurden, hängt damit nicht von einer Auswahl bestimmter Anlassdelikte oder verfahrensführender Stellen ab. Sie ist somit repräsentativ für die in diesen vier Bundesländern durchgeführten Verfahren mit Verkehrsdatenabfragen. Eine Verallgemeinerung auf die Bundesrepublik ist ohne wesentliche Einschränkungen möglich, da bei der Auswahl der Bundesländer darauf geachtet wurde ggf. vorhandene kriminalpolitische, strukturelle (Stadt- und Flächenstaaten) und historische (alte versus neue Bundesländer) Unterschiede proportional nahezu ausgewogen zu erfassen.

Die Repräsentativität wird auch nicht dadurch geschmälert, dass statt der ursprünglich anvisierten 600 Akten nur 467 in die Auswertung eingingen, da es nicht zu systematischen Ausfällen kam. Einzig die statistische Trennschärfe bezüglich Differenzen zwischen unterschiedlichen Gruppen ist dadurch etwas reduziert.[420]

III. Fragebogenkonzeption

Um die in den Akten enthaltenen Informationen in einer Form zu erfassen, die eine statistische Analyse erlaubt, wurden ein Fragenkatalog und ein darauf abgestimmtes Eingabeprogramm erstellt. Entsprechend der komplexen Struktur der Akten selbst ist dieser in verschiedene Teile gruppiert, die miteinander verknüpft sind. Dabei konnte auf die Erfahrungen des Projekts zur „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen“[421] zurückgegriffen werden.

Grundlage des Fragebogens sind die vier Haupttabellen Verfahren (V), Beschuldigte (B), Beschluss (S) und Anschluss (A). Jeder dieser Blöcke wird durch einen eigenen Fragenkomplex erfasst. Abgesehen von der Tabelle Verfahren werden die Tabellen innerhalb einer Akte ggf. mehrfach ausgefüllt. Die Module sind in besonderer Weise miteinander verknüpft. V steht in 1-n-Verknüpfungen zu B und S, S wiederum in 1-n-Verknüpfung zu A. In einem (1) Verfahren kann es also mehrere (n) Beschuldigte und mehrere (n) Beschlüsse geben und ein Beschluss kann sich auf mehrere (n) Anschlüsse beziehen.



Ferner sind drei zusätzliche Tabellen eingefügt, die sich auf mehrere Haupttabellen beziehen und ergänzende Detailangaben ermöglichen. Sie sind also mit mehreren der

416 Jedem Datensatz in den nach den vier Ländern getrennten Tabellen, die jeweils die Daten aller TK-Anbieter enthielten, wurde eine gleich verteilte Zufallszahl zwischen 0 und 1 zugeordnet. Alle Datensätze, deren Zufallszahl kleiner als die Auswahlquote war, wurde gezogen.

417 Es wurden mehr Beschlüsse als die notwendigen 150 Beschlüsse gezogen, um die erwartbaren Ausfälle auszugleichen. Tatsächlich waren einige Verfahren nicht verfügbar, in selteneren Fällen konnte auch ein GS-Aktenzeichen nicht zugeordnet werden.

418 Prinzipiell ist dies möglich, da ein Beschluss – wie die Aktenanalyse zeigt – im Schnitt etwa drei TK-Anbieter betrifft. Allerdings hängt das Auftreten solcher Duplikate stark von der Auswahlquote ab. Je geringer diese ist, desto seltener treten Duplikate auf.

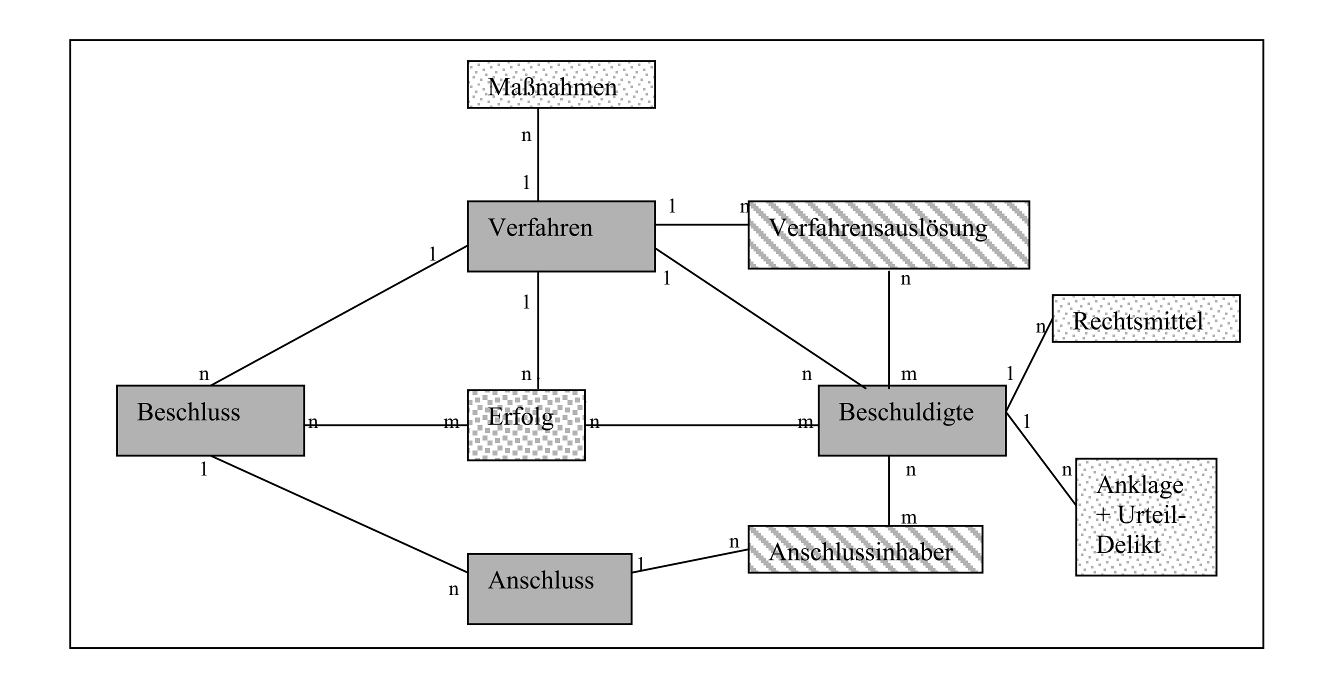
419 Dies war möglich, da bei ca. einem Drittel der Beschlüsse nicht das Aktenzeichen des Verfahrens sondern nur das GS-Aktenzeichen der Beschluss fassenden Stelle verzeichnet war.

420 So können z. B. prozentuale Differenzen zwischen alternativen Gruppen auf der Ebene der Verfahren im schlechtesten Fall erst ab einer Differenz von 6,5 Prozent anstatt von 5,7 Prozent als statistisch gesichert angesehen werden.

421 *Albrecht/Dorsch/Krüpe*, 2003.

Haupttabellen verbunden, um sicherzustellen, dass der Zusammenhang der erfassten Angaben erhalten bleibt. Dabei kommt es immer darauf an, welche Informationen den Akten entnommen werden können. Eine dieser zusätzlichen Tabellen ist die Tabelle „Verfahrensauslösung". Soweit dies möglich war, wurden die Angaben zum verfahrensauslösenden Sachverhalt nicht nur auf das Verfahren, sondern auch bezogen auf die einzelnen Beschuldigten ausgefüllt. Zwischen Anschluss und Beschuldigtem gibt es eine Tabelle „Anschlussinhaber". Anschlussinhaber kann der Beschuldigte, aber auch ein Dritter sein. Diese Tabelle war nur für die Beschuldigten auszufüllen, gegen die der Beschluss gerichtet ist. Dies ermöglicht es, die Beziehung jedes Beschuldigten zum jeweiligen Anschlussinhaber gesondert zu erfassen. Um Erfolge zuordnen zu können, wurde die Tabelle „Erfolg" mit den Tabellen Beschluss, Verfahren und Beschuldigte verknüpft. Als Erfolge wurden beispielsweise die Ermittlung des aktuellen Aufenthaltsortes des Beschuldigten bzw. seines Mobiltelefons, Hinweise auf die Täterschaft, die Erweiterung des Tatvorwurfes, Hinweise auf weitere Tatbeteiligte, die Sicherung von Beweisen, usw. behandelt. Dadurch werden Erfolge in zweierlei Hinsicht erfasst. Zum einen können sie durch die 1-n Anbindung zu der Tabelle Verfahren als Erfolge des „Gesamtverfahrens" aufgenommen werden, insbesondere in den Fällen, in denen eine Zuordnung zur jeweiligen Maßnahme und zum Beschuldigten nicht möglich ist. Darüber hinaus ist es aber – sofern nach Aktenlage feststellbar – auch möglich, den eingetretenen Erfolg einer bestimmten Maßnahme nach §§ 100g, 100h StPO und damit einem bestimmten Beschluss zuzuordnen. Dies geschieht durch die Verbindung zwischen Erfolg und Beschluss. Da nicht zwingend ein Erfolg mehreren Maßnahmen zuzuordnen sein muss und umgekehrt nicht eine Maßnahme immer mehrere Erfolge aufzuweisen hat, besteht zwischen diesen Modulen eine n-m Verbindung. Jeder Erfolg kann somit keiner Maßnahme, einzelnen oder mehreren Maßnahmen zuzuordnen sein, jede Maßnahme kann keinen Erfolg, einzelne oder mehrere Erfolge erzielt haben. Darüber hinaus wurde „Erfolg" auch in n-m Verknüpfung mit „Beschuldigte" gesetzt, damit, sofern dies feststellbar ist, aufgenommen werden kann, hinsichtlich welches Beschuldigten ein Erfolg herbeigeführt werden konnte.

Aus Gründen der Übersichtlichkeit und aus auswertungsökonomischen Gründen wurden weitere Themenkomplexe aus den Haupttabellen herausgenommen. So wurden die Telekommunikationsanbieter-Daten-unabhängigen Ermittlungsmaßnahmen in der Tabelle Maßnahmen aus der Tabelle Verfahren ausgegliedert. So konnte jede einzelne Ermittlungsmaßnahme, die in dem Verfahren angeordnet wurde, erfasst werden. Eine weitere – diesmal aus „Beschuldigte" – ausgegliederte Tabelle stellt „Anklage+ Urteil-Delikt" dar. Nur so konnten alle einzelnen Delikte, die dem Beschuldigten zur Last gelegt wurden und ihre Entwicklung im weiteren Verfahren erfasst werden. Auch die Tabelle „Rechtsmittel" gehört zum Beschuldigten. Da aber mehrere Rechtsmittel eingelegt worden sein können, wurden die Angaben zum Rechtsmittel aus der Beschuldigtentabelle herausgenommen.



IV. Durchführung

1. Aktenanforderung

Die Anbieter verfügten zu einem großen Teil lediglich über die „Gs-Aktenzeichen“, da sie nur von der ermittlungsrichterlichen Anordnung oder staatsanwaltschaftlichen Eilanordnung betroffen sind und dementsprechend auch nur von dieser Kenntnis hatten. Durch diesen Umstand kam es zu erheblichen zeitlichen Verzögerungen bei der Aktenanforderung. Die Staatsanwaltschaften mussten zunächst die Gs-Aktenzeichen den Verfahrensaktenzeichen zuordnen. Dies geschah teilweise bei der Staatsanwaltschaft selbst. Andere Staatsanwaltschaften mussten zunächst bei den Gerichten um Auskunft bitten, welches Verfahrensaktenzeichen zu dem jeweiligen Gs-Aktenzeichen gehört. Teilweise wurde die Zuordnung als nicht möglich deklariert. Nachdem dann die Gs-Aktenzeichen den Verfahren zugeordnet worden waren, mussten die Akten erst in den jeweiligen Abteilungen angefordert werden. In den meisten Fällen erfolgte die Aktenübermittlung postalisch.

Zwischen Aktenanforderung und Zusendung der Akten vergingen in den Bundesländern Baden-Württemberg und Nordrhein-Westfalen im Schnitt vier bis fünf Wochen, in Mecklenburg-Vorpommern durchschnittlich sechs Wochen und in Berlin etwa zwei bis drei Monate. Dies resultiert wohl daraus, dass es in Berlin nur eine Staatsanwaltschaft und eine Amtsanwaltschaft gibt und in Mecklenburg-Vorpommern lediglich vier Staatsanwaltschaften. Insofern entfiel in diesen Bundesländern eine hohe Anzahl von Akten auf die einzelnen Staatsanwaltschaften.

Zum Teil konnten die Gs-Aktenzeichen keinem Verfahren zugeordnet werden. Zudem waren einige der von den Telekommunikationsanbietern erfassten Js-Aktenzeichen laut Staatsanwaltschaft nicht existent. Eine nicht unbeträchtliche Anzahl von Verfahren war noch nicht abgeschlossen oder eine Einsichtnahme war aus anderen Gründen nicht möglich. In diesen Fällen erfolgte eine weitere Ziehung von Aktenzeichen. Die Gesamtstichprobe beläuft sich somit auf 800 Aktenzeichen.

2. Dateneingabe

Der Auswertung im Rahmen der Aktenanalyse liegen insgesamt 467 Strafakten zugrunde. Die Auswertung erlaubt eine sichere Beantwortung der eingangs aufgeworfenen Fragestellungen, da die der Analyse zugrundeliegende Aktenauswahl keine Verzerrungen enthält, die die Verteilungen mehr als marginal beeinflussen. Die Auswertung der Akten erfolgte überwiegend in den Räumen des Max-Planck-Instituts. Zu einem geringen Anteil war es notwendig, die Aktenanalyse bei der jeweiligen Staatsanwaltschaft vor Ort vorzunehmen. Die Auswertung der Akten erfolgte durch studentische Hilfskräfte (Studentinnen und Studenten der Rechtswissenschaft). Die Akteninhalte wurden direkt in ein Access-Formular eingegeben. Zur Gewährleistung der einheitlichen Aktenauswertung wurden die studentischen Mitarbeiter umfassend in die Fragestellungen eingeführt. Ferner wurde zur Sicherung übereinstimmender Auswertung eine Fragebogenkommentierung erstellt. Zudem fanden regelmäßige Besprechungen zwischen den Projektmitarbeitern statt. Zu Beginn wurden alle Eingaben kontrolliert und die Akte mit dem jeweiligen Bearbeiter besprochen. Im weiteren Verlauf wurden die Akten stichprobenartig überprüft. Eine übergreifende Kontrolle der Eingabe erfolgte über eine Datenmaske.

Die Bearbeitungsdauer variierte je nach Umfang des Verfahrens. Im Durchschnitt betrug die Bearbeitungszeit vier Stunden für einen Aktenumfang von durchschnittlich etwa 400 Seiten. Für kleinere Akten (ca. 50 Seiten) wurde eine Stunde zur Aktenauswertung benötigt, für größere (ca. 3 000 Seiten) erreichte die Auswertungszeit bis zu 14 Stunden. Die statistische Auswertung der Daten erfolgte mit dem Statistikprogramm SPSS (Statistical Package for the Social Sciences).

D. Expertengespräche

I. Einführung

Expertengespräche mit Praktikern aus allen Bereichen, die mit Maßnahmen nach §§ 100g, 100h StPO (aus unterschiedlichen Perspektiven) konfrontiert werden, sollen die Ergebnisse der schriftlichen Befragung und der Aktenanalyse vertiefen und zur Auslotung der Interpretationsspielräume dienen. Interviews wurden mit Richtern, Staatsanwälten, Strafverteidigern, Polizisten, Mitarbeitern von Telekommunikationsunternehmen und Datenschutzbeauftragten aus den Ländern Baden-Württemberg, Berlin, Mecklenburg-Vorpommern und Nordrhein-Westfalen durchgeführt.

II. Fragebogenkonzeption

Für die Expertengespräche wurde für die verschiedenen Berufsgruppen je ein Interviewleitfaden entwickelt. Schwerpunktmäßig sind die folgenden Themenkomplexe in den Interviews angesprochen worden:

- Durchführung der Maßnahme nach §§ 100g, 100h StPO
- Richtervorbehalt
- Verhältnismäßigkeit und Subsidiaritätsgrundsätze
- Schwierigkeiten zwischen den Beteiligten
- Benachrichtigung und zeugnisverweigerungsberechtigte Betroffene
- Verfahren und Rechtsmittel
- Erfolge der Verkehrsdatenabfrage
- Verhältnis zu und Vorteile gegenüber anderen Ermittlungsmaßnahmen
- Zukünftige Gestaltung der Maßnahme und Reform der strafprozessualen Grundlagen

Die Fragenkomplexe wurden je nach Tätigkeitsfeld an den Interviewpartner und die einzelnen Berufsgruppen angeglichen.

III. Durchführung

Die Expertengespräche wurden in den Bundesländern Baden-Württemberg, Berlin, Mecklenburg-Vorpommern und Nordrhein-Westfalen geführt. Bei der Auswahl der Gesprächspartner wurden die unterschiedlichen Arbeitsbereiche der einzelnen Berufsgruppen berücksichtigt. Im Falle der Richter wurden Ermittlungsrichter interviewt. Die in den Expertengesprächen befragten Staatsanwälte waren in den Schwerpunktdezernaten Organisierte Kriminalität, Betäubungsmittelkriminalität und Computerkriminalität eingesetzt. Interviewte Polizisten waren der Kriminalpolizei (Schwerpunkte Betäubungsmittelkriminalität, Organisierte Kriminalität, Computerkriminalität) und den Landeskriminalämtern zugeordnet. Bei den Strafverteidigern wurden Anwälte, die über Erfahrungen mit Betäubungsmittelkriminalität und Revisionen verfügen, ausgewählt. Interviews mit Mitarbeitern von Telekommunikationsunternehmen betrafen solche, die Aktenzeichen der Anordnungen zur Verfügung gestellt haben (Arcor, Eplus, o_2, T-Com, T-Mobile, Vodafone). Zudem wurden Mitarbeiter der vier Datenschutzbeauftragten der Bundesländer, aus denen die Akten angefordert wurden, befragt. Insgesamt wurden mit 53 Personen Interviews geführt. Die Interviews wurden teilweise telefonisch, teilweise auch „face to face“ geführt. Die Gesprächsdauer betrug dabei zwischen 20 Minuten und zwei Stunden. Die Gespräche wurden in Form von Ergebnissen zu den einzelnen Fragen protokolliert und einer qualitativen Analyse unterzogen.

4. Ergebnisse der empirischen Untersuchung

A. Struktur und Eingriffsbreite von Verkehrsdatenabfragen

I. Verkehrsdatenabfragen im Spiegel von Telekommunikationsunternehmensdaten

Die für die Stichprobenziehung erhobenen Telekommunikationsanbieterdaten erlauben allgemeine Analysen zur Struktur, zum Umfang und zur Eingriffsbreite der verschiedenen Typen der Verkehrsdatenabfrage. Aus den an ein Telekommunikationsunternehmen (Mobilfunknetz, Marktanteil ca. 15 Prozent, etwa zwölf Millionen Kunden) gerichteten Beschlüssen und den hieraus resultierenden Abfrageergebnissen, die einen Zeitraum von drei Monaten erfassen, lässt sich ein repräsentatives Bild allgemeiner Kennziffern der Verkehrsdatenabfrage ermitteln. Ein weiterer Datensatz bezieht sich auf den Festnetzbereich und Nordrhein-Westfalen (2004). Aus ihm können Informationen zu Deliktsstrukturen im Zusammenhang mit Verkehrsdatenabfragen (und hier auch zur Abfrage von Bestandsdaten zu dynamischen IP-Adressen) entnommen werden.

In dem Auswertungszeitraum von drei Monaten (Januar bis März 2003) wurden an das betroffene Telekommunikationsunternehmen 1 714 Auskunftsersuchen gestellt. Auf das Jahr 2003 bezogen handelte es sich somit um etwa 7 000 Auskunftsersuchen. Die Abfragen sind fast ausschließlich auf die Vergangenheit gerichtet. Nur in seltenen Fällen (0,7 Prozent) bezieht sich eine Verkehrsdatenabfrage ausschließlich auf die Zukunft. Etwas häufiger sind kombinierte, Zukunft und Vergangenheit der Verbindungen erfassende Abfragen zu beobachten (5 Prozent).

Im Festnetzbereich Nordrhein-Westfalens kam es 2004 zu 1 926 Abfragen. Diese bezogen sich ganz überwiegend auf die Feststellung abgehender Kontakte. In 3 Prozent der Fälle wurden ankommende Telefonnummern abgefragt. Etwa 22 Prozent der Anfragen betrafen (dynamische) IP-Adressen.

II. Die Struktur der Verkehrsdatenabfrage und ihrer Erledigung

Die Art der Verkehrsdatenabfrage wird durch das Unternehmen in A-, B- und C-Suchläufe unterschieden. Ein A-Suchlauf zielt auf die Identifizierung von Telefonnummern, die von einem Kunden des Mobilfunknetzes angewählt worden sind. Der B-Suchlauf bezieht sich auf den Nachweis von Verbindungen, die aus dem Mobilfunknetz zu einer im Beschluss genannten Nummer hergestellt worden sind. Der C-Suchlauf enthält die Feststellung von Verbindungen, die in einer oder mehreren im Beschluss angesprochenen Funkzellen entstanden sind, betrifft also die Funkzellenabfrage, die zu den eigentlichen Verkehrsdaten räumliche Daten hinzufügt. Die Verteilung der Abfragen lässt einen eindeutigen Schwerpunkt bei der Identifizierung von Verbindungen, die zu einer, den Strafverfolgungsbehörden bereits bekannten, Telefonnummer bestanden haben, erkennen. Etwa 60 Prozent der Beschlüsse betreffen den so genannten Zielsuchlauf, mit dem das Telekommunikationsunternehmen alle gespeicherten Kundendaten darauf hin untersucht, ob Verbindungen zu einer oder mehreren im Beschluss bezeichneten Telefonnummern hergestellt worden sind. Etwa 18 Prozent der Beschlüsse beziehen sich auf eine Funkzellenabfrage.

Die Bearbeitungsdauer (Zeitpunkt der Abfrage bis Abgang der Auskunft) ist im Durchschnitt kurz. 96 Prozent der Anfragen sind innerhalb einer Woche erledigt. Der Mittelwertvergleich zeigt für Funkzellenabfragen einen erhöhten Wert von etwas mehr als vier Tagen. Demgegenüber liegt die Bearbeitungsdauer für Zielwahlsuchläufe und Kombinationen zwischen Zielwahlsuche und der Kundentelefonabfrage bei durchschnittlich zweieinhalb Tagen (AB, B, Tabelle 4).

Tabelle 4

Bearbeitungsdauer in Tagen

Abfrageart	Mittelwert	N	Std. Abweichung
A	3,58	12	2,429
AB	2,55	334	4,428
B	2,81	991	4,041
C	4,30	295	2,791
Insgesamt	**3,03**	**1 632**	**3,966**

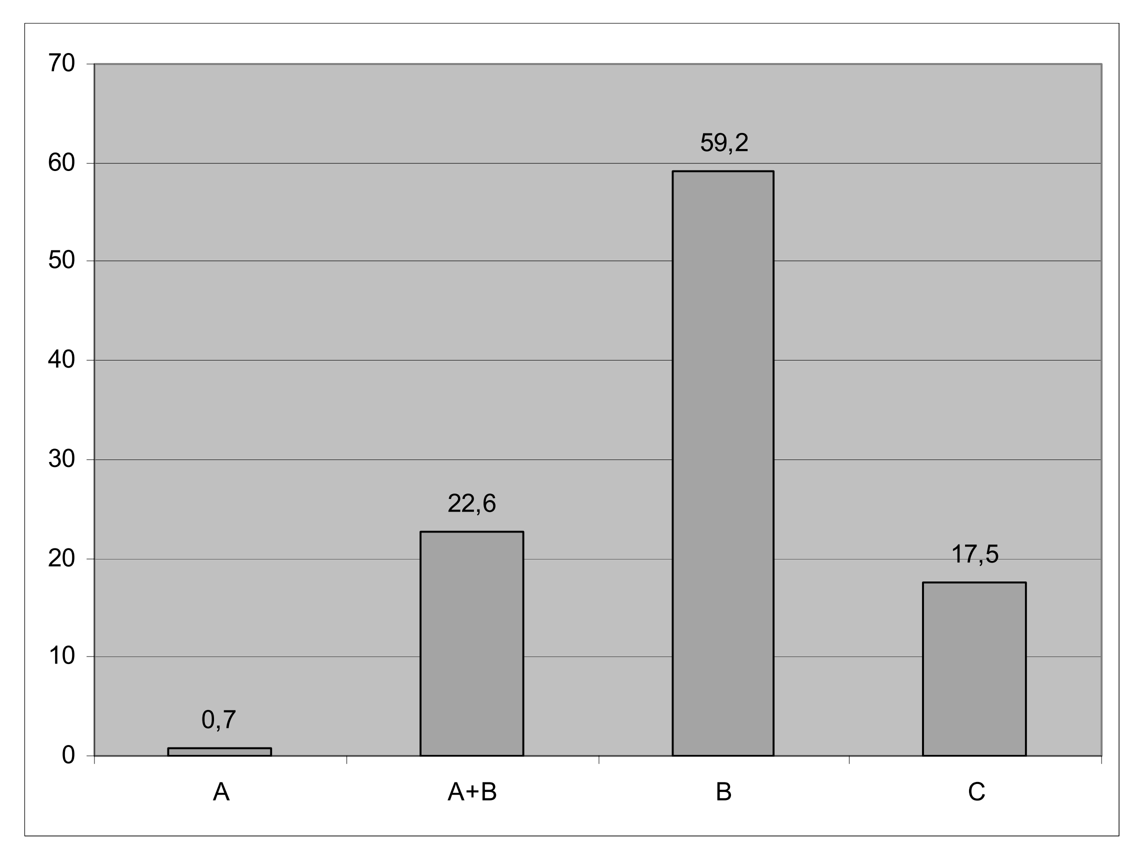
Vor allem aus der Perspektive der Beurteilung der Vorratsspeicherung ist dann von Bedeutung, für welche Zeiträume vor der Abfrage in der Praxis nach Verkehrsdaten nachgefragt wird. Die Verkehrsdatenabfrage bezieht sich auf einen Zeitraum, der durchschnittlich 26 Tage vor dem Zeitpunkt des Anfrageschreibens beginnt. Etwa die Hälfte der Abfragen betrifft einen Zeitraum von vier Tagen oder weniger. Dabei unterscheidet sich die Reichweite in die Vergangenheit nach der Art der Abfrage. Grundsätzlich kann wohl davon ausgegangen werden, dass sich die Praxis der Abfrage an die (durch Rechnungsstellung begründete) Speicherungsdauer der Telekommunikationsunternehmen angepasst hat. In diesem Fall war die Speicherungsdauer von Transaktionsdaten von dem Unternehmen auf 80 Tage festgelegt worden. Tatsächlich beziehen sich knapp 20 Prozent der Verkehrsdatenabfragen auf einen Abfragebeginn, der offensichtlich an dem Löschzeitpunkt orientiert ist (zwischen 76 und 80 Tage). Nur vereinzelt (0,6 Prozent) erstrecken sich Abfragen (auch) auf nach dem Löschzeitpunkt liegende Zeiten (wobei diese Abfragen in der Regel auch innerhalb der löschfreien Zeit liegende Zeiträume abdecken).

Die Abfragen von Verbindungen aus einem bekannten Telefonanschluss (kombiniert mit Zielwahlsuchen) legen den Beginn der Abfrage am engsten an den Löschzeitpunkt. Hier sind es knapp 60 Prozent der Abfragen, die nach Daten von bis zu zwischen 75 und 80 Tagen vor dem

Abbildung 11



Art der Verkehrsdatenabfrage in Prozent



Anschreiben an das Telekommunikationsunternehmen verlangen. Im Falle von Zielwahlsuchen liegen im Bereich von 75 und mehr Tagen etwa 9 Prozent der Anfragen und bei Funkzellenabfragen betrifft dieser Zeitraum noch einen Fall (0,3 Prozent). Demnach dürfte ein Bedarf nach längerer Speicherung vor allem bei Überwachungen bekannter Telefonanschlüsse und insoweit bei bereits bekannten Tatverdächtigen vorhanden sein. Freilich deckt sich eine zunehmende Ausdehnung in die Vergangenheit auch mit einer zunehmenden Überwachungsdauer. Denn aus der Reichweite der Verkehrsdatenabfrage in die Vergangenheit lässt sich gut die Dauer der Abfrage vorhersagen. Eine Regression des erwarteten Abfragebeginns auf die Dauer der Abfrage zeigt einen sehr starken (und linearen) Zusammenhang und einen entsprechend hohen Anteil an erklärter Varianz.

Je länger in die Vergangenheit eine Verkehrsdatenabfrage reicht, desto eher ist sie offensichtlich auf eine allgemeine Erforschung der Kommunikation eines Tatverdächtigen (und der Kommunikationspartner) gerichtet. Zielwahlsuche und Funkzellenabfrage antworten demgegenüber auf stärker konkretisierte Fragestellungen, die sich, so ist anzunehmen, unmittelbar aus den ersten Ermittlungsschritten ergeben.

Tabelle 5

Vorhersage Dauer aus gewünschtem Beginn bei A/B-Abfragen

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,663	,440	,438	788,19686

a Predictors: (Constant), Eingangsdatum – gewünschter Beginn der Abfrage.

III. Die Dauer der Überwachung

Die verschiedenen Arten von Abfragen lassen deutliche Unterschiede in der Zeitspanne, für die Daten erhoben werden, erkennen. Die Funkzellenabfrage ist auf kurze Zeiträume ausgerichtet. Ihre durchschnittliche Dauer liegt bei fünf Stunden. Freilich fallen bereits knapp ein Viertel der Funkzellenabfragen unter eine Stunde; das Maximum liegt bei knapp drei Tagen. Auch der Zielsuchlauf konzentriert sich auf kurze Zeiträume. Davon heben sich solche Verkehrsdatenabfragen nachdrücklich ab, die (auch) die Erhebung von Daten aus einem bekannten Anschluss beinhalten (A, AB, Tabelle 6).

Die Unterschiede werden in der graphischen Darstellung (Abbildung 12) noch deutlicher. Die Abfrage von einem überwachten Anschluss abgehender Verbindungen wird selten gezielt auf einen kurzen Zeitraum eingesetzt. Hier liegt der Ermittlungsansatz sichtlich auf einer breit angelegten Erfassung der Kommunikationsverkehrsdaten eines Tatverdächtigen (oder Nachrichtenmittlers). Der Schwerpunkt liegt bei zwei bis drei Monaten. Zielwahlsuchen und Funkzellenabfragen setzen den Schwerpunkt im Stunden- und Minutenbereich.

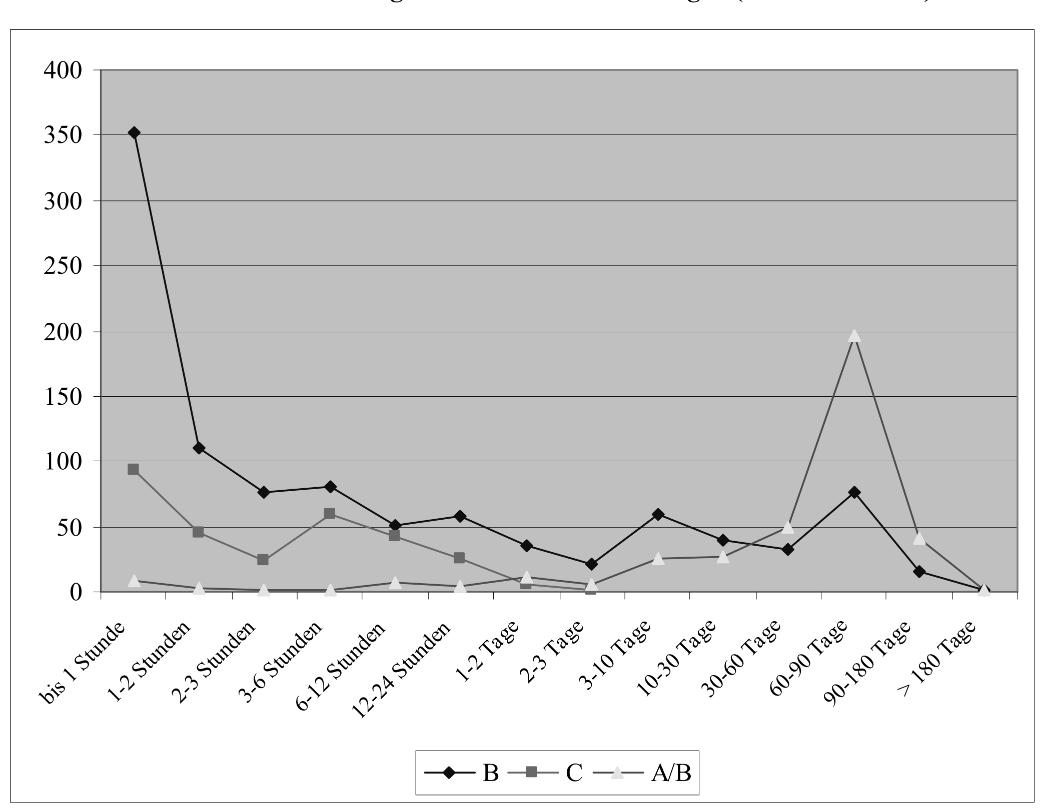
Tabelle 6

Überwachungsdauer in Stunden

Art des Suchlaufs	Mittelwert	N	Std. Abweichung
A	1 248	12	790
AB	1 511	383	1 051
B	261	1 010	694
C	5	297	7
Insgesamt	**505**	**1 702**	**921**

Abbildung 12

Dauer der Datenerhebung bei verschiedenen Abfragen (absolute Zahlen)



IV. Resultate der Verkehrsdatenabfrage

Die Ergebnisse der Verkehrsdatenabfrage, gemessen daran, ob überhaupt Mitteilungen über Verkehrsdaten vorgenommen wurden, sind erwartungsgemäß. Die aus unterschiedlichen Perspektiven weit angelegten Abfrageformen der Funkzellenabfrage und der abgehenden Kommunikation eines überwachten Anschlusses resultieren ganz überwiegend in der Übermittlung von Transaktionsdaten an die Strafverfolgungsbehörden. Lediglich 17 aus 299 Funkzellenabfragen (5,6 Prozent) und 106 aus 386 kombinierten Zielwahlsuchen und Anschlussüberwachungen (27,5 Prozent) führen zu der Information, dass keine Verkehrsdaten aus dem abgefragten Bereich und Zeitraum registriert worden sind. Die Zielwahlsuche selbst läuft erwartungsgemäß in der Regel ins Leere. Nur 154 (15 Prozent) von 1 015 Zielwahlsuchen liefern den Strafverfolgungsbehörden aus dem angefragten Unternehmen Ergebnisse in Form von Verbindungen aus dem Mobilfunknetz zu einem in der Anfrage benannten Anschluss. Die Quote entspricht im Übrigen etwa dem Marktanteil des Unternehmens und spricht demnach auch dafür, dass sich die Klientel der Strafverfolgungsbehörden wohl (durchschnittlich) marktkonform verhält.

Tabelle 7

Abfrageart und Ergebnisse in Form der Übermittlung von Transaktionsdaten

Abfrageart	Ergebnis der Abfrage		Insgesamt
	Keine Daten geliefert	Daten geliefert	
A	3	9	12
AB	106	280	386
B	861	154	1 015
C	17	282	299
Insgesamt	**987**	**725**	**1 712**

V. Die Eingriffsbreite der Verkehrsdatenabfrage

Die Eingriffsbreite der Verkehrsdatenabfrage kann neben der Dauer der Überwachung durch die Anzahl der überwachten Anschlüsse sowie durch die Anzahl der (unterschiedlichen) registrierten Kommunikationspartner beschrieben werden. Einen Überblick enthält die nachstehende Tabelle 8.

Geht man von der insgesamt erfassten Kommunikation aus, dann liegt die Kombination von Zielwahlsuche und Überwachung eines bestimmten Anschlusses vorne. Durchschnittlich werden hier Transaktionsdaten zu 623 Gesprächen (oder Kontakten) erfasst. Freilich ist der Mittelwert beeinflusst durch zwei Extremwerte, deren Eliminierung allerdings immer noch zu einem Durchschnitt von 357 Gesprächen pro Abfrage führt. Die Zielwahlsuche registriert (wenn überhaupt ein Kontakt registriert worden ist) durchschnittlich 20 Kontakte. Für Funkzellenabfragen enthält Tabelle 8 die Information, dass im Durchschnitt Verkehrsdaten zu 286 Kontakten angefallen sind.

Die Eingriffsbreite wird jedoch erst dann vollständig sichtbar, wenn die Kommunikationskontakte auf die Anzahl hierin einbezogener unterschiedlicher Personen hin untersucht werden. Aus dem vorliegenden Datensatz wurden die Telefonnummern abgehender und ankommender Kommunikation auf unterschiedliche Anschlüsse reduziert, um darstellen zu können, wie viele Personen (gemessen an unterschiedlichen Telefonnummern) durch verschiedene Formen der Verkehrsdatenabfrage registriert werden (Tabelle 9).

Die Abfrage von Funkzellen führt durchschnittlich zu der Registrierung abgehender Gespräche von 111 (verschiedenen) Mobilfunkteilnehmern und durchschnittlich 183 (unterschiedlichen) Telefonnummern, die eingehende Kommunikation repräsentieren. Die Standardabweichung ist erheblich. Dies reflektiert die durch Ort und Zeit bedingten Unterschiede im Mobilfunkaufkommen.

In der nachstehenden Abbildung 13 werden die in verschiedenen Tages- und Nachtzeiten platzierten Funkzellenabfragen von bis zu einer Stunde präsentiert. Hieraus erfolgt eine erwartbare Verteilung. In den Nachtstunden zwischen 0.00 und etwa 6.00 Uhr geht die Telekommunikation auf fast Null zurück.

Abbildung 14 stellt den Telekommunikationsverlauf auf der Grundlage einer Funkzellenabfrage für den inneren Bereich einer Kleinstadt über 24 Stunden dar.

Tabelle 8

Mittelwert erfasster Gespräche und abgefragter Telefonnummern/Funkzellen bei verschiedenen Arten der Verkehrsdatenabfrage

Art der Abfrage		Alle Gespräche	Anrufe	Überwachte Nummern bzw. Funkzellen
AB	Mittelwert	623 (357)	134	1,4
	N	281 (279)	204	387
	Std. Abweichung	4 039 (624)	240	1,1
B	Mittelwert		20	1,3
	N		153	1 014
	Std. Abweichung		65	0,9
C	Mittelwert	286		3,2
	N	282		299
	Std. Abweichung	574	.	1,9
Insgesamt	Mittelwert	**463**	**85**	**1,7**
	N	**572**	**358**	**1 712**
	Std. Abweichung	**2 871**	**194**	**1,4**

Tabelle 9

Durch Funkzellenabfragen erfasste unterschiedliche Anschlüsse

		Verschiedene A-Teilnehmer	Verschiedene B-Teilnehmer
N	Valid	282	282
	Missing	17	17
Mittelwert		111	183
Median		50	64
Std. Abweichung		168	347
Varianz		28 189	120 170
Range		1 280	3 456
Summe		**31 463**	**51 648**

Abbildung 13

Durchschnittlich erfasste Kontakte bei Funkzellenabfragen mit einer Dauer von bis zu einer Stunde

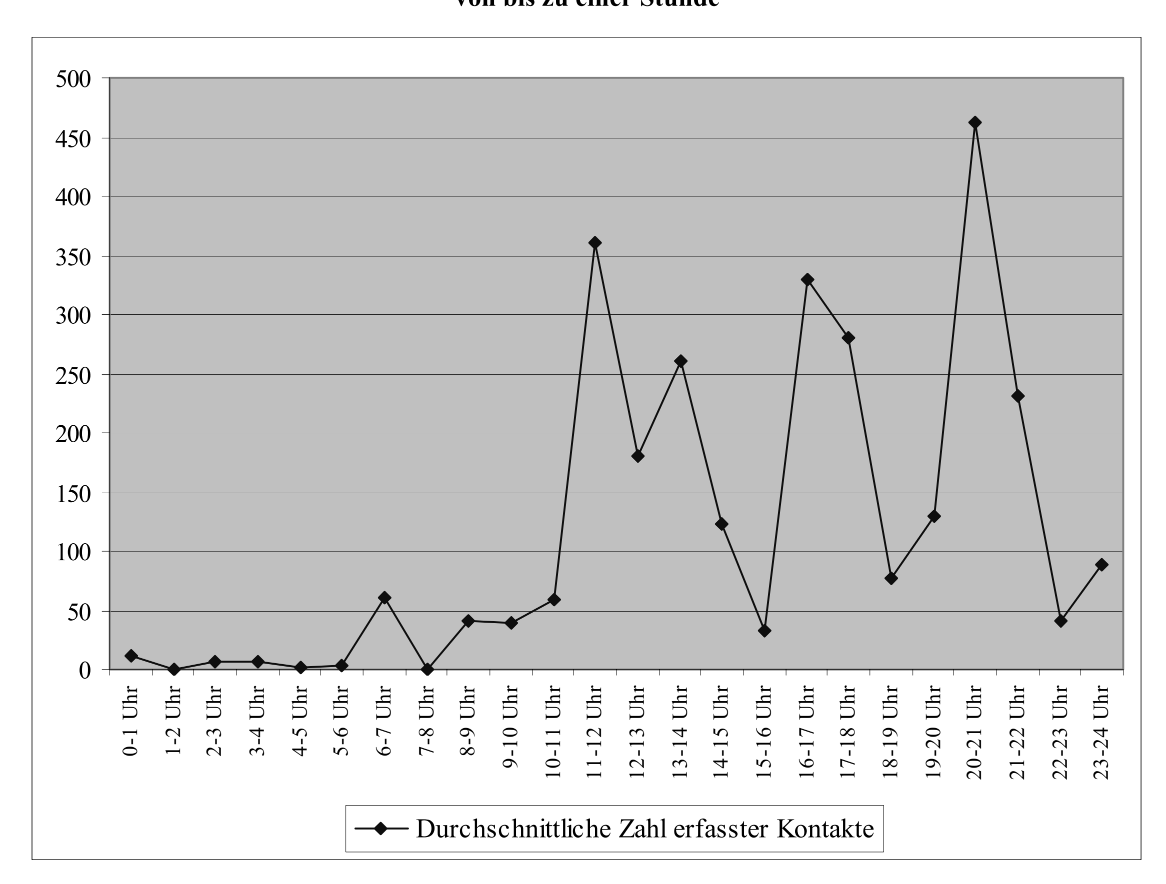
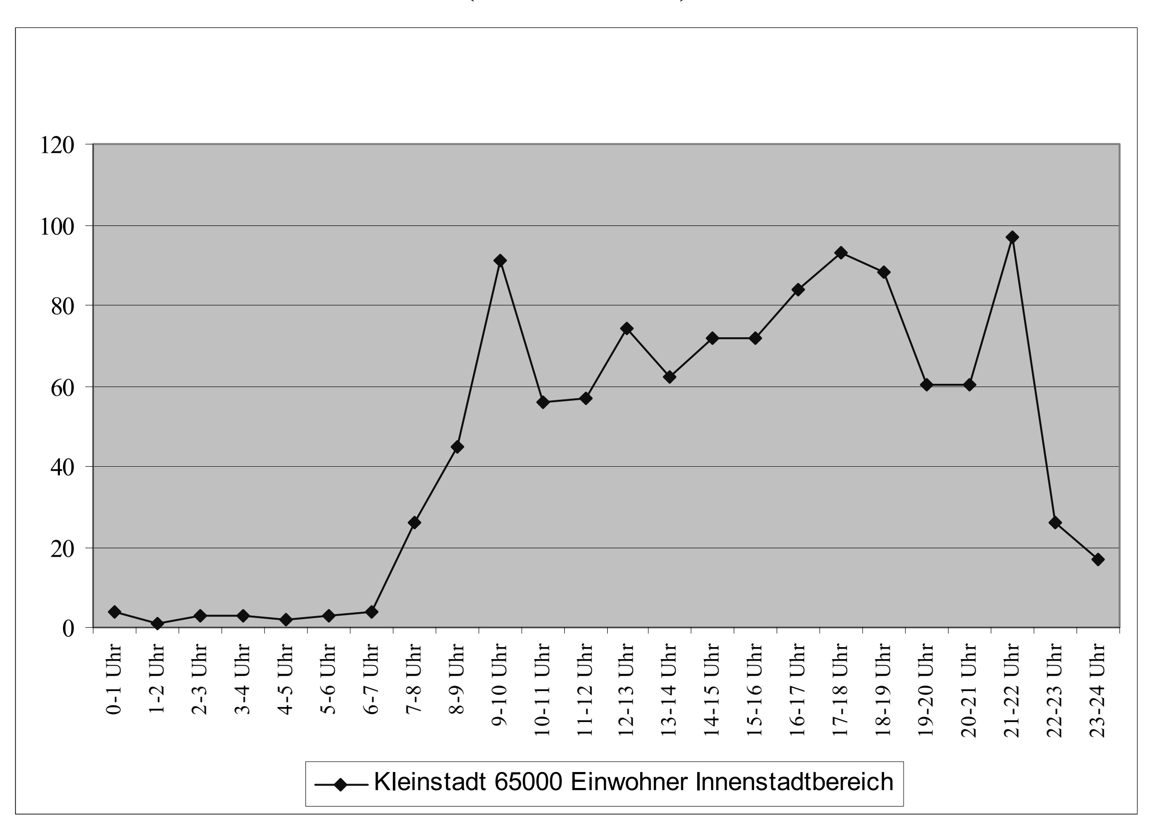


Abbildung 14

Durchschnittlich pro Stunde erfasste Kontakte in der Funkzellenabfrage des innerstädtischen Bereichs einer Kleinstadt (65 000 Einwohner)



Mit den Funkzellenabfragen wurden in einem Zeitraum von drei Monaten und in dem erfassten Bundesland Daten über etwa 83 000 Verbindungen mit (innerhalb einer Funkzellenabfrage) unterschiedlichen Anschlüssen erfasst. Somit dürften innerhalb eines Jahres allein durch Funkzellenabfragen bei einem einzelnen Telekommunikationsunternehmen bis zu 250 000 Kommunikationsteilnehmer mit Informationen über Ort, Zeit, Dauer und Partner der Kommunikation registriert worden sein. Durch die Funkzellenabfrage waren im Jahr 2005 in Deutschland insgesamt demnach etwa 2 Prozent der Mobilfunkteilnehmer betroffen, wenn Zeitraum und Unternehmen die durchschnittliche Praxis der Funkzellenabfrage repräsentieren.

Weitaus enger ist das Ergebnis zur Erfassungsbreite der Zielwahlsuche. Durch die (erfolgreiche) Zielwahlsuche werden im Durchschnitt 2,5 Kommunikationspartner erfasst. Im überwiegenden Teil der Zielwahlsuchen handelt es sich um einen Partner (60 Prozent). Mehr als zehn Kommunikationspartner werden in 4 Prozent der Fälle registriert (Tabelle 10).

In der Überwachung konkreter Anschlüsse (in Kombination mit Zielwahlsuchen) fallen erwartungsgemäß erhebliche Verkehrsdatenmengen an. In Tabelle 11 sind die zentralen Informationen enthalten. Schließt man die bereits weiter oben erwähnten Extremfälle (N = 2) aus, dann sind durch diese Form der Verkehrsdatenabfrage in einem Zeitraum von 3 Monaten knapp 12 000 Kommunikationspartner und knapp 100 000 Kontakte registriert worden.[422]

[422] N x Mittelwert ohne Extremfälle (siehe Zeilen 1 und 3, Klammerwerte).

Tabelle 10

Zielwahlsuche und Registrierung von Kommunikationsteilnehmern

Anzahl	N	% Insgesamt	% bei Ergebnis	% kumuliert
1	91	*9,0*	*59,5*	*59,5*
2	25	*2,5*	*16,3*	*75,8*
3	9	*,9*	*5,9*	*81,7*
4	8	*,8*	*5,2*	*86,9*
5	3	*,3*	*2,0*	*88,9*
6	5	*,5*	*3,3*	*92,2*
7	2	*,2*	*1,3*	*93,5*
9	3	*,3*	*2,0*	*95,4*
11	1	*,1*	*,7*	*96,1*
12	3	*,3*	*2,0*	*98,0*
13	2	*,2*	*1,3*	*99,3*
21	1	*,1*	*,7*	*100,0*
Insgesamt	**153**	***15,1***	***100,0***	
Ohne Ergebnis	861	*84,9*		
Insgesamt	**1 014**	***100,0***		

Tabelle 11

Registrierte Kommunikationspartner und Anzahl der Kontakte bei der Abfrage abgehender Kommunikation

		Verschiedene Partner	Anzahl der Kontakte
N	Valid	281 (279)	281 (279)
	Missing	106	106
Mittelwert		197 (43)	623 (357)
Median		22	116 (115)
Mode		1	2
Std. Abweichung		2 159 (67)	4 039 (624)
Varianz		4 665 365 (4 502)	16 310 361 (389 673)
Range		35 336 (617)	66 732 (4 673)
Minimum		1	1
Maximum		35 337 (618)	66 733 (4 674)
Insgesamt		**55 461 (11 952)**	**175 085 (99 469)**

VI. Deliktsstruktur und Verkehrsdatenabfrage im Festnetzbereich

Die Deliktsstruktur bei Abfragen im Festnetzbereich ist in dem hier erfassten Zeitraum und Land eindeutig durch den Betrug bestimmt. Zwar lassen die Daten des Telekommunikationsunternehmens eine Differenzierung kaum zu. Doch spielen Betrugshandlungen, die über eine telefonische Kontaktaufnahme vorbereitet werden, eine gewisse Rolle (Enkeltrick).

Bemerkenswert sind dann die Anteile von Betäubungmittel-, Raub- und Morddelikten. Besonders herausgehoben sind im Übrigen Drohungsdelikte (unter denen § 241 StGB sowie § 126 StGB zusammengefasst wurden.

Die Verkehrsdatenabfrage hat damit jedenfalls in Nordrhein-Westfalen Schwerpunkte im Bereich der Kapitaldelikte sowie bei Straftaten, die unter Verwendung von Kommunikationsmitteln begangen werden und bei denen wohl die Kontaktspuren in Form der Transaktionsdaten der Telekommunikation einen wesentlichen Ansatz in den Ermittlungen herstellen.

Erwartungsgemäß bildet die Abfrage von Bestandsdaten zu dynamischen IP-Adressen eine andere Deliktsstruktur ab. Die Deliktsstruktur ist ferner davon abhängig, ob der Anteil an den IP-Adressenabfragen zugrunde gelegt, oder ob von dem Anteil an allen abgefragten IP-Adressen ausgegangen wird. So spielen Kinderpornografieverfahren keine erhebliche Rolle, wenn ihr Anteil an den IP-Abfragen insgesamt betrachtet wird. Auf Kinderpornografieverfahren entfallen freilich fast 30 Prozent der insgesamt abgefragten IP-Adressen.

Abbildung 15

Delikte bei Abfragen im Festnetzbereich (Nordrhein-Westfalen, 2004)

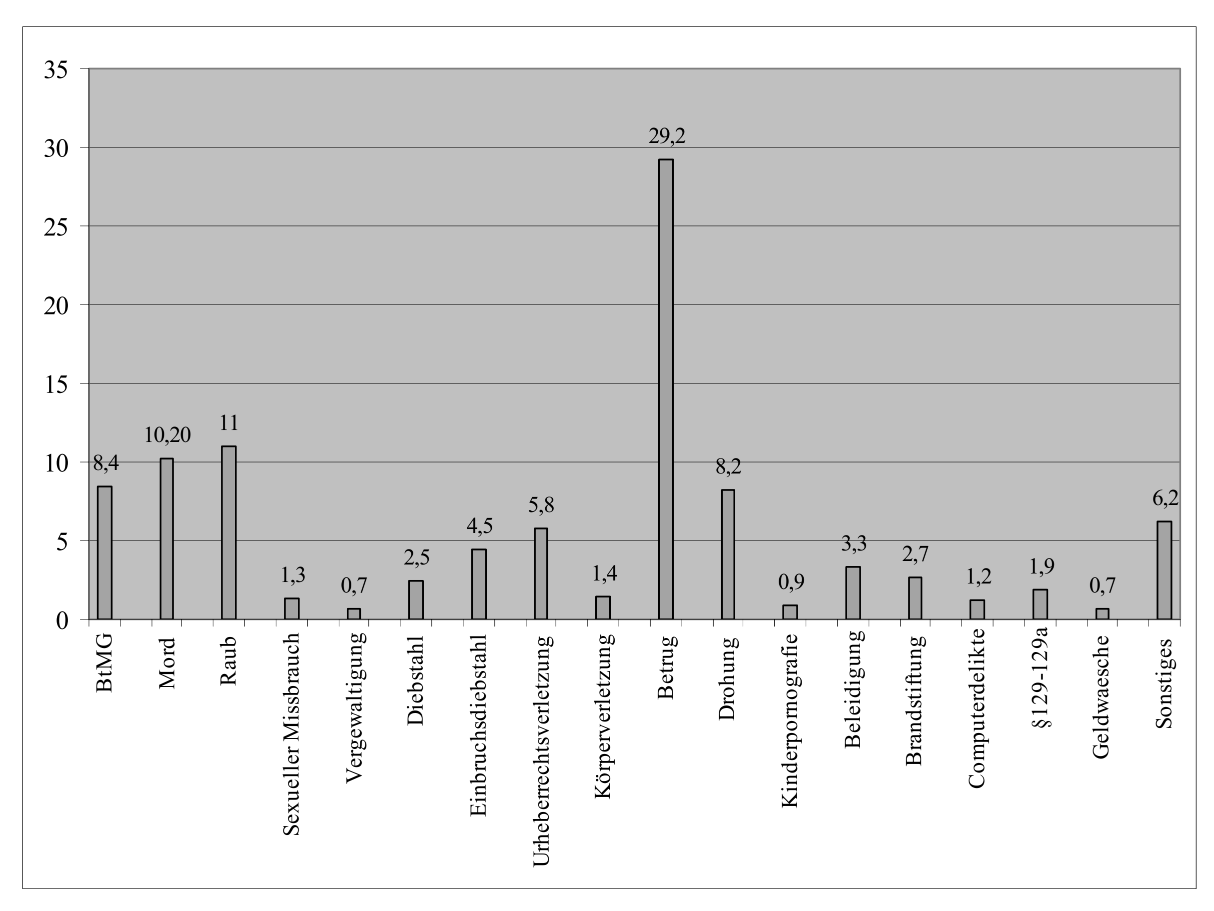
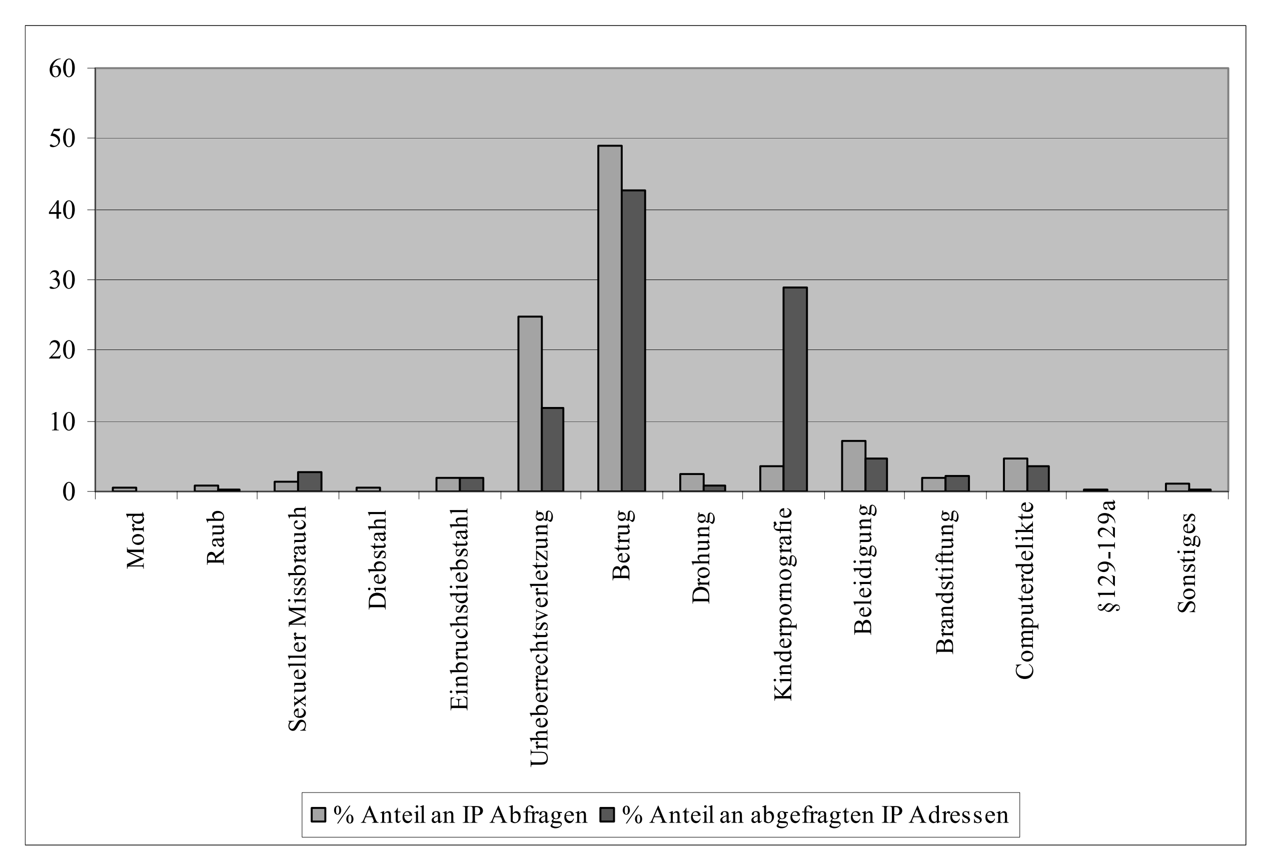


Abbildung 16





B. Grunddaten der Aktenanalyse und Befragungen

I. Aktenanalyse

Der Aktenauswertung liegen 467 Verfahren zugrunde. Die Anzahl der Verfahren verteilt sich etwa gleich auf die vier Bundesländer, aus denen die Akten angefordert wurden. 27 Prozent der Verfahren stammen aus Baden-Württemberg, 22 Prozent aus Berlin, 27 Prozent aus Mecklenburg-Vorpommern und 24 Prozent aus Nordrhein-Westfalen.

1. Verfahren, Beschlüsse, Anschlüsse und Beschuldigte

Wie in Abbildung 17 dargestellt folgen aus 467 Verfahren 1257 Beschlüsse zur Abfrage von Verkehrsdaten. Diese Beschlüsse betrafen 1909 Anschlüsse, denen wiederum 1645 Anschlussinhaber zugeordnet werden konnten.

Bei 181 Verfahren handelte es sich um Verfahren gegen unbekannte Täter. Die übrigen Verfahren betrafen 697 Beschuldigte. Abbildung 18 zeigt den Anteil der Verfahren gegen Unbekannt. In 39 Prozent der Verfahren konnten der oder die Täter nicht identifiziert werden.

Die Anzahl der Beschlüsse nach §§ 100g, 100h StPO pro Verfahren variiert von einem Beschluss bis zu 35. Am häufigsten wurde die Verkehrsdatenabfrage einmal pro Verfahren angeordnet (56 Prozent der Verfahren). Zwei Beschlüsse wurden in 18 Prozent der Verfahren und drei Beschlüsse in 9 Prozent der Verfahren erlassen. Durchschnittlich sind pro Verfahren 2,7 Beschlüsse ergangen. Betroffene Anschlüsse pro Verfahren gab es bis zu 76. Am häufigsten war jedoch auch hier die Abfrage der Daten von einem Anschluss (48 Prozent der Verfahren). Zwei Anschlüsse wurden in 17 Prozent der Verfahren abgefragt und drei Anschlüsse in 9 Prozent der Verfahren. Im Mittel wurden zu 4,1 Anschlüssen pro Verfahren Verkehrsdaten abgefragt. Pro Beschluss wurden Daten zu einem bis zu zwölf Anschlüssen übertragen. Auch hier war jedoch die Abfrage von Daten eines Anschlusses am häufigsten (78 Prozent der Beschlüsse). Im Durchschnitt wurden Daten zu 1,5 Anschlüssen pro Beschluss erhoben.

Entlang der Bundesländer liegen Unterschiede hinsichtlich der Anzahl der pro Verfahren erlassenen Beschlüsse vor. Während in Baden-Württemberg im Mittel 2,8, in

Abbildung 17

Grundgesamtheiten

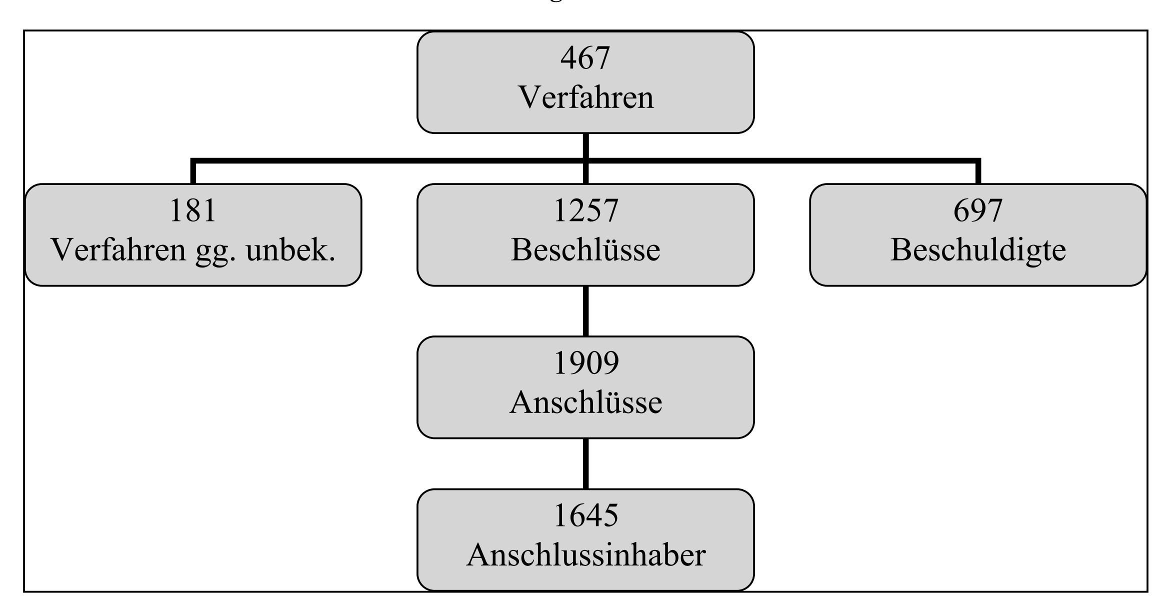
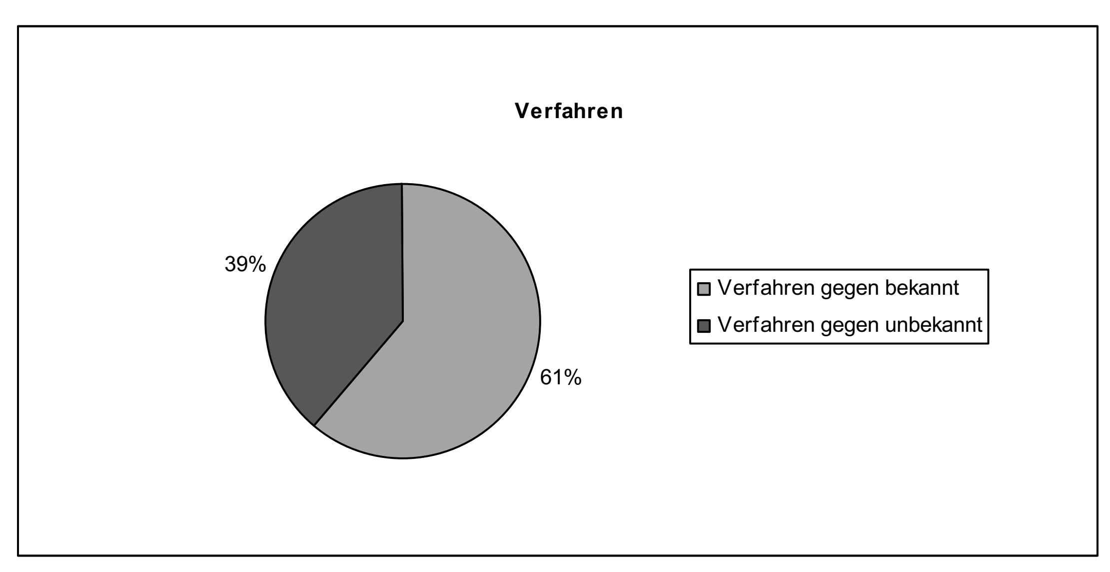


Abbildung 18

Anteil der Verfahren gegen unbekannt



Berlin 1,9 und in Mecklenburg-Vorpommern 1,6 Beschlüsse erlassen wurden, wurden in Nordrhein-Westfalen im Mittel 4,2 Beschlüsse pro Verfahren ausgefertigt. Der Unterschied kann durch unterschiedliche Anordnungsmodalitäten hervorgerufen werden. So erlässt die Praxis teilweise für jeden Anschluss bzw. pro Anbieter einen neuen Beschluss, während in anderen Regionen sämtliche Anbieter und alle Anschlüsse in *einem* Beschluss aufgeführt werden. Auf die zugrundeliegenden Delikte bezogen werden bei Tötungs- und Betäubungsmitteldelikten mehr Beschlüsse in einem Verfahren erlassen als bei anderen Delikten. So ergibt sich aus den Akten, dass bei Tötungsdelikten durchschnittlich 6,4 Beschlüsse und bei Betäubungsmitteldelikten 3,7 Beschlüsse ausgefertigt wurden. Bei anderen Delikten wurden zwei bis drei Beschlüsse erlassen.

2. Art der Anschlüsse

Von den Verkehrsdatenabfragen waren verschiedene Arten von Anschlüssen betroffen. Tabelle 12 kann entnommen werden, in welchem Umfang bei welcher Anschlussart Verkehrsdaten abgefragt wurden.

Zu zwei Dritteln wurden ein- oder abgehende Daten von oder zu Mobilfunkanschlüssen erhoben (66 Prozent). 25 Prozent der betroffenen Anschlüsse waren private Festnetzanschlüsse. Betriebliche Festnetzanschlüsse waren dagegen nur zu 3,8 Prozent Ziel der Maßnahmen. Fax und E-Mail waren sehr selten betroffen. Voice over IP-Dienste (Internet-Telefonie) wurden in keiner Akte erwähnt.

Abbildung 19 differenziert zwischen Abfragen von Daten, die eine Rufnummer betreffen und solchen, bei denen eine Kennung (z. B. IMEI-Nummer oder IP-Adresse) Gegenstand des Beschlusses ist.

Am häufigsten sind Rufnummern Gegenstand der Abfrage (87 Prozent der Anschlüsse). Bei 103 Anschlüssen (5 Prozent der Anschlüsse) konnte den Akten explizit entnommen werden, dass es sich um ISDN-Anschlüsse handelte. Zu diesen ISDN-Anschlüssen gehörten bis zu 15 Rufnummern. Am häufigsten waren jedoch drei Rufnummern pro ISDN-Anschluss (43 Prozent der ISDN-Anschlüsse). Abfragen zu IMEI-Nummern erfolgten bei 10 Prozent der Anschlüsse. Dabei handelte es sich um

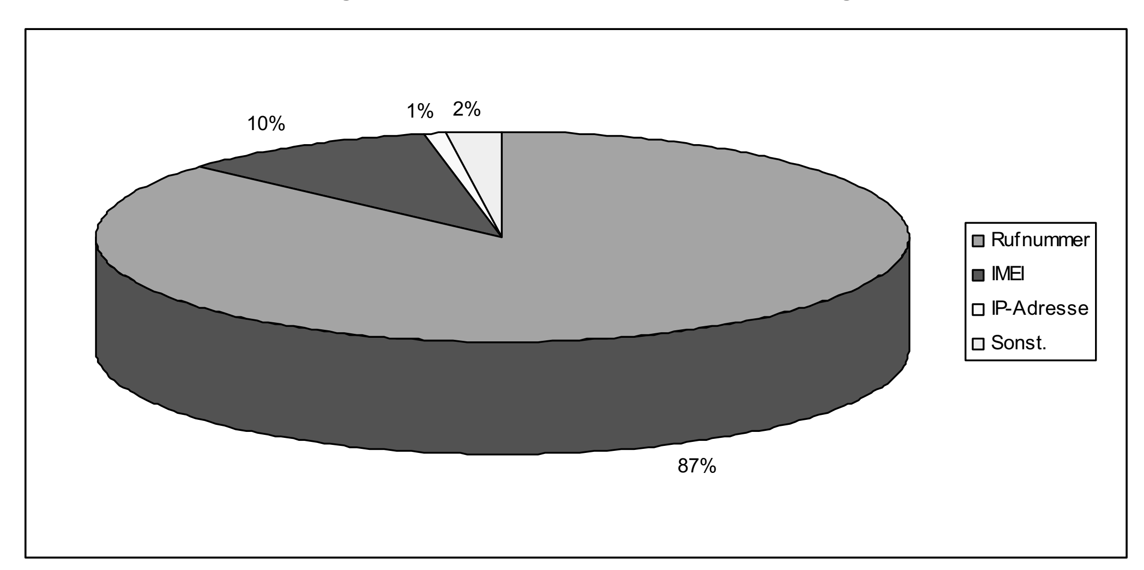
Tabelle 12

Art der Anschlüsse

	Anzahl	Prozent
Festnetz privat	478	*25,0%*
Festnetz Betrieb	72	*3,8%*
Mobiltelefon	1 258	*65,9%*
Öffentlicher Anschluss	32	*1,7%*
Fax	2	*0,1%*
e-mail	7	*0,4%*
Andere WWW-Dienste	3	*0,2%*
Sonstige oder nicht ersichtlich	57	*3,1%*
Total	**1 909**	***100,0%***

Abbildung 19

Abfrage von Daten zu Rufnummern oder Kennungen



Abfragen von bis zu 15 IMEI-Nummern pro Beschluss. Am häufigsten wurden die Daten zu einer IMEI-Nummer abgefragt (88 Prozent dieser Fälle). Abfragen zu IP-Adressen erfolgten bei 1 Prozent der Anschlüsse (14 Fälle). Sonstige Abfragen (2 Prozent) betrafen u. a. PUK- und Super-Pin, Prepaid-Karten-Seriennummern, IMSI-Nummern und E-Mail-Accounts.

3. Arten der Verkehrsdatenabfrage

Wie bereits ausgeführt beziehen sich Abfragen auf verschiedene Arten von Verkehrsdaten. Unterschieden werden die Abfrage von vorhandenen Daten, die Abfrage von zukünftig anfallenden Daten, die Zielwahlsuche und die Funkzellenabfrage in Abgrenzung zur Standortabfrage. Die verschiedenen Abfragearten wurden häufig gleichzeitig angeordnet. Wie sich die verschiedenen Arten der Verkehrsdatenabfrage auf die in den Akten befindlichen Beschlüsse verteilen, lässt sich Abbildung 20 entnehmen.

In den Beschlüssen wurden überwiegend (93 Prozent) bereits gespeicherte Daten abgefragt. Die Zielwahlsuche wurde in 55 Prozent der Beschlüsse angeordnet. In die Zukunft gerichtet waren 33 Prozent der Abfragen. Standortabfragen (18 Prozent) wurden etwa doppelt so häufig angeordnet wie Funkzellenabfragen (10 Prozent der Fälle)[423]. Bei den sonstigen Abfragen (4 Prozent) handelte es sich u. a. um Abfragen der Rufnummer zur IMEI-Nummer, Auskünfte zur benutzten SIM-Karte sowie um Bestandsdaten.

Welche Arten der Verkehrsdatenabfrage gleichzeitig angeordnet wurden, lässt sich für die häufigsten Arten der Abfrage Abbildung 21 entnehmen. Die Abfrage von vorhandenen Daten wurde zu 56 Prozent mit Zielwahlsuchen und zu 30 Prozent mit in die Zukunft gerichteten Abfragen kombiniert. Zukünftige anfallende Daten wurden zu 84 Prozent zusammen mit vorhandenen Daten abgefragt oder zusammen mit Zielwahlsuchen (57 Prozent) angeordnet. Mit der Zielwahlsuche wurde fast immer die Abfrage von vorhandenen Daten kombiniert (94 Prozent). Funkzellenabfragen erfolgten zu 86 Prozent zusammen mit der Abfrage von vorhandenen Daten. Die Standortabfrage wurde ganz überwiegend zusammen mit der Abfrage von vorhandenen Daten (92 Prozent), weniger stark ausgeprägt mit der Zielwahlsuche (53 Prozent) oder mit der Abfrage von zukünftigen Daten (45 Prozent) angeordnet.

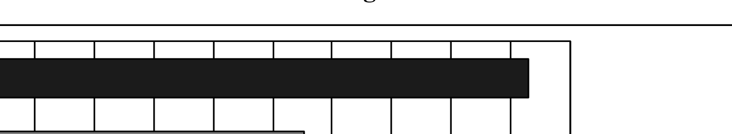
Für die drei Hauptarten der Verkehrsdatenabfrage (Abfrage vorhandener Daten, Abfrage zukünftiger Daten, Zielwahlsuche) wurde festgestellt, dass in 35 von insgesamt 1257 Beschlüssen keine und in 380 Beschlüssen eine der drei Abfragearten vorkam. Bei 651 Beschlüssen wurden zwei dieser Hauptarten gleichzeitig und in 191 Beschlüssen alle drei gleichzeitig angeordnet.

Abbildung 22 zeigt, welche Katalogdelikte mit welchen Arten von Verkehrsdatenabfragen verfolgt wurden[424].

[423] Dabei ist zu berücksichtigen, dass die Standortabfrage nur bei expliziter Erwähnung in den Akten aufgenommen wurde. Bei allgemeiner Anordnung der Abfrage von Verkehrsdaten, bei der sie theoretisch erfasst sein könnte, wurde dies nicht als Standortabfrage bewertet.

[424] Die übrigen Katalogdelikte und auch weitere sonstige Straftaten wurden nicht aufgeführt, da der Aussagegehalt wegen der geringen Anzahl von Fällen eingeschränkt ist.

Abbildung 20



Arten der Verkehrsdatenabfragen in den Beschlüssen

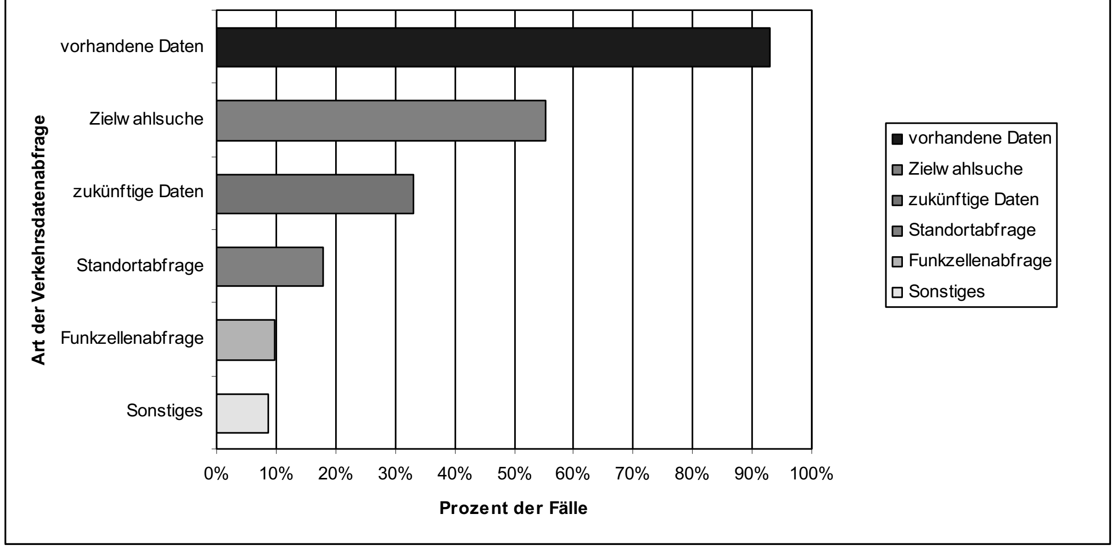


Abbildung 21



Gleichzeitige Anordnung der verschiedenen Abfragearten

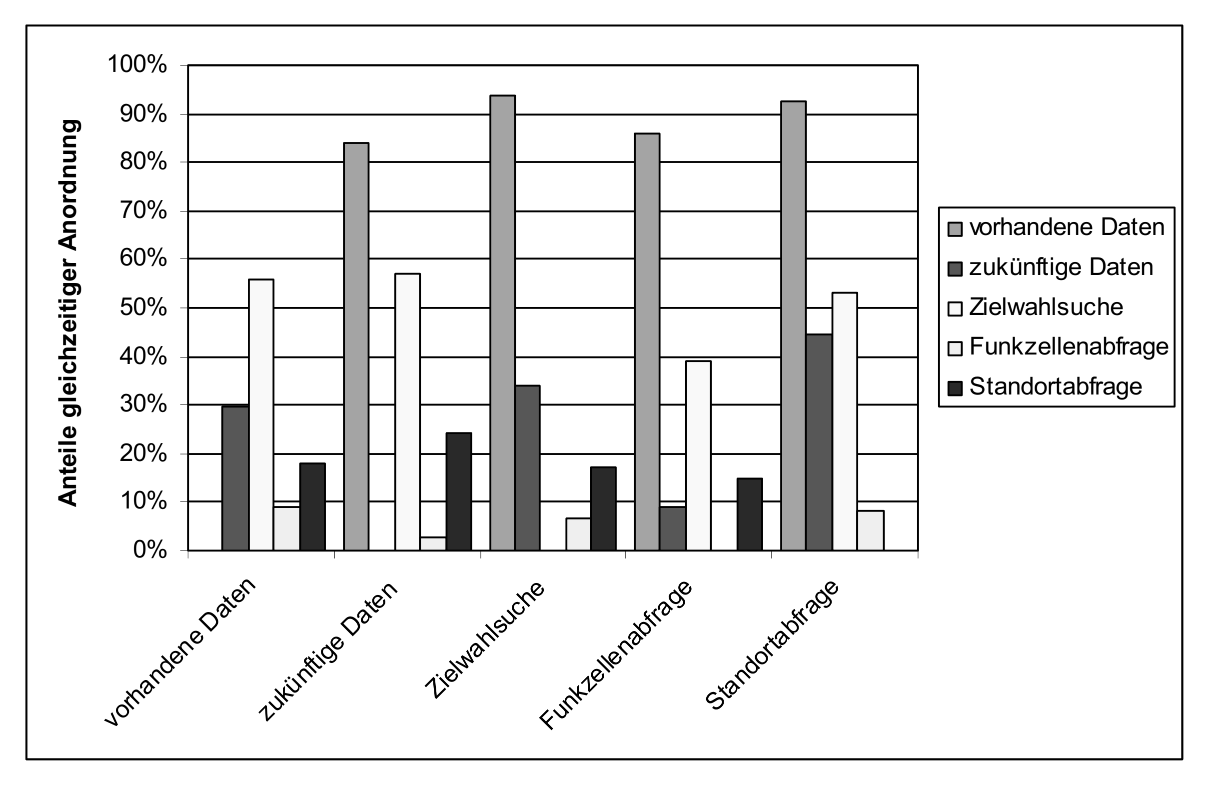
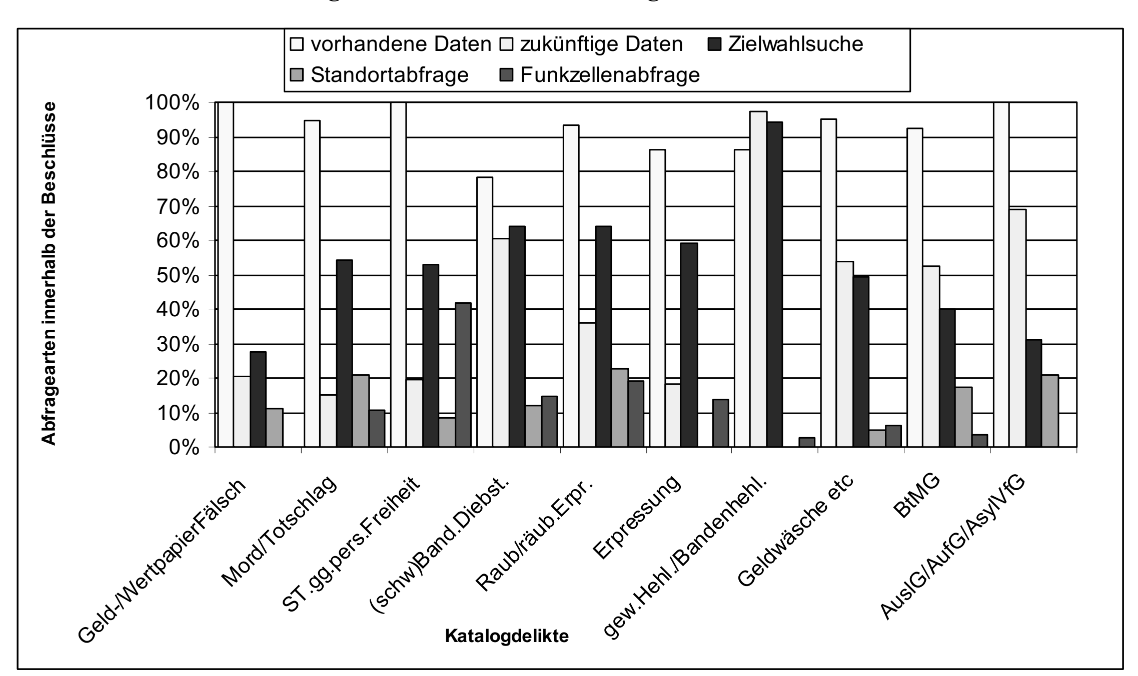


Abbildung 22

Art der Abfrage differenziert nach Katalogdelikten in den Beschlüssen

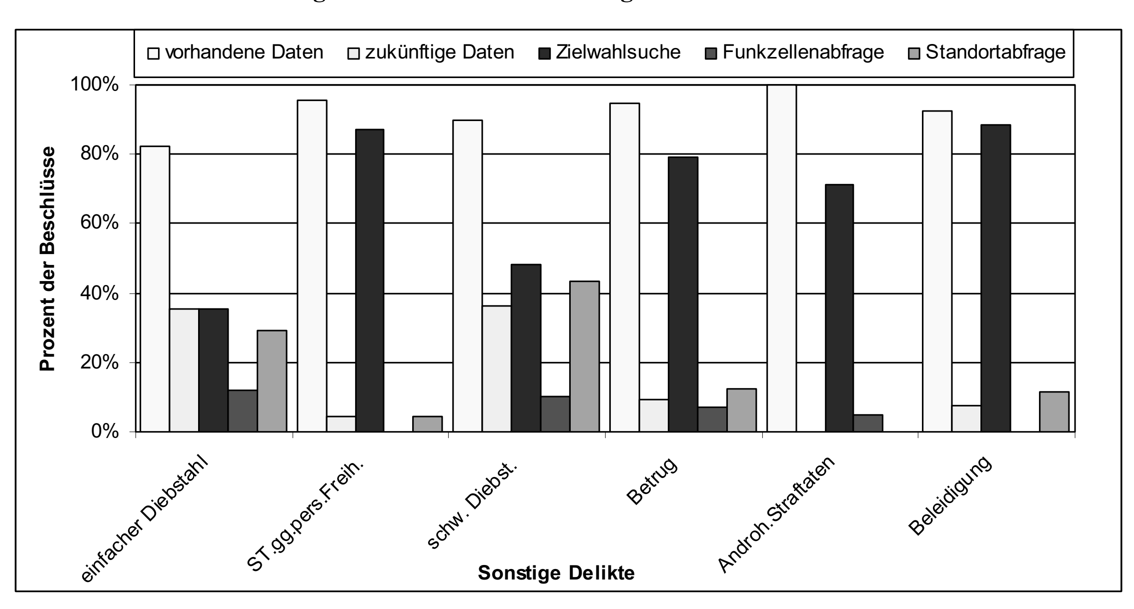


Bei allen Delikten wurde zu 80 bis 100 Prozent die Abfrage vorhandener Verkehrsdaten angeordnet. Die Zielwahlsuche und die Abfrage zukünftiger Daten erfolgte häufiger bei der Verfolgung gewerbsmäßiger Hehlerei als bei anderen Straftaten. Bei Straftaten gegen die persönliche Freiheit sowie bei Raub bzw. räuberischer Erpressung wird relativ oft eine Funkzellenabfrage durchgeführt. Die Standortabfrage wird vor allem bei Tötungsdelikten, Raub bzw. räuberischer Erpressung und bei Verstößen gegen das AuslG angeordnet.

Auch bei den sonstigen Delikten (Abbildung 23) werden wiederum am häufigsten (zwischen 80 und 100 Prozent) vorhandene Verkehrsdaten abgefragt. Die Zielwahlsuche ist vor allem bei Straftaten gegen die persönliche Freiheit wie Bedrohung oder Nötigung durch einen Anrufer, bei Beleidigungen mittels Endeinrichtung und Betrugsdelikten (z. B. Enkeltrick) die angewandte Abfrageart. Die Funkzellen- und die Standortabfrage kommen häufig beim einfachen und schweren Diebstahl zur Anwendung.

Abbildung 23

Art der Abfrage differenziert nach sonstigen Delikten in den Beschlüssen



4. Anzahl der verpflichteten Anbieter

In 3095 Fällen wurden Diensteanbieter durch 1 257 Beschlüsse gemäß §§ 100g, 100h StPO zur Übermittlung von Daten verpflichtet. Von einem Beschluss sind damit durchschnittlich knapp drei Telekommunikationsformen betroffen. Bei 42 Prozent der Anschlüsse wurde lediglich ein Anbieter zur Auskunft verpflichtet. Vier Anbieter waren zu 11 Prozent mit der Abfrage der Daten beauftragt, während zwei (7 Prozent) und drei (8 Prozent) verpflichtete Anbieter seltener vorkamen. Bei 9 Prozent der Beschlüsse wurden fünf Telekommunikationsunternehmen zur Auskunft verpflichtet. In 6 Prozent der Beschlüsse wurden pauschal „alle, die geschäftsmäßig Telekommunikationsdienste erbringen“ zur Auskunft verpflichtet. Seltener waren die Verpflichtung von sechs (4 Prozent), sieben (1 Prozent), acht (1 Prozent) und neun (3 Prozent) Anbietern sowie die Verpflichtung des „jeweils zuständigen Netzbetreibers“ (1 Prozent).

In allen Bundesländern konzentrierte sich die Auskunftsverpflichtung auf einen Diensteanbieter. Im Übrigen sind jedoch Unterschiede entlang der Bundesländer festzustellen. In Baden-Württemberg kommt es zu Schwerpunkten mit der Verpflichtung von vier oder fünf Anbietern in einer Anordnung, während in Berlin drei oder neun Anbieter im Vordergrund standen. In Berlin hängt die hohe Zahl gleichzeitig Verpflichteter mit dort etablierten regionalen Anbietern zusammen. So ist z. B. Sitz der Gesellschaft des häufig verpflichteten Anbieters BerliKomm in Berlin und auch das Hauptstadtbüro von BT Ignite befindet sich in Berlin. In Nordrhein-Westfalen und Mecklenburg-Vorpommern befindet sich ein Schwerpunkt der Verpflichtungen bei vier Anbietern. In Mecklenburg-Vorpommern sind zudem Anordnungen für „alle, die geschäftsmäßig Telekommunikationsdienste erbringen“ gängig.

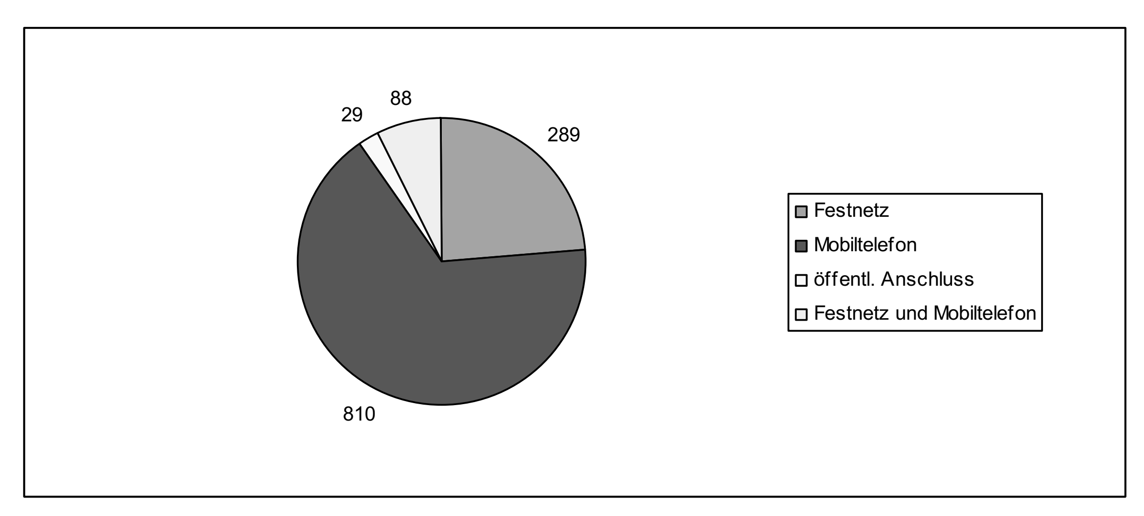
Der am häufigsten verpflichtete Anbieter der in die Untersuchung fallenden Beschlüsse ist Vodafone (60 Prozent der Fälle). T-Mobile rangiert mit 54 Prozent an zweiter Stelle. Eplus war in 42 Prozent der Fälle der Verpflichtete und o2 in 38 Prozent der Fälle. Die Konzentration der Verpflichtungen auf Mobilfunkanbieter lässt sich mit der Zunahme der Telekommunikation über Mobilfunkgeräte erklären. Wie Abbildung 24 zeigt, betrafen die Beschlüsse zu zwei Dritteln Mobiltelefone.

T-Com ist mit 34 Prozent der Fälle der am häufigsten zur Abfrage der Verkehrsdaten verpflichtete Festnetzbetreiber. Arcor wurde in 8 Prozent der Fälle zur Auskunft verpflichtet. Im Übrigen wurden auch mehrere kleinere Unternehmen durch die Beschlüsse betroffen, wie Colt Telecom (5 Prozent), Berlikomm (4 Prozent) und BT Ignite (4 Prozent; sonstige: 8 Prozent). In 6 Prozent der Fälle war die Anordnung pauschal an „alle“ Anbieter adressiert und in 1 Prozent der Fälle an den jeweils zuständigen Netzbetreiber.

Abbildung 24



Art der betroffenen Telefonarten bei den Beschlüssen



5. Ermittlungsdelikte in den Verfahren

Den ausgewerteten Verfahren lagen unterschiedliche Ermittlungsdelikte zugrunde. In Abbildung 25 wird die Häufigkeit der Delikte dargestellt.

Etwa 23 Prozent der Verfahren liegen zwei oder mehr Delikte zugrunde. Im Vordergrund stehen Ermittlungen wegen Raubdelikten und (räuberischer) Erpressung (26 Prozent, N = 119) und Diebstahl (23 Prozent, N = 110). In jeweils etwa 15 Prozent der Verfahren waren Betrug (N = 64) und Rauschgiftdelikte (N=62) Anlass für die Einleitung des Ermittlungsverfahrens. Seltener waren Straftaten gegen die persönliche Freiheit (N = 31) und Tötungsdelikte (N = 27) sowie Körperverletzungen (N = 21) und Beleidigungen (N = 21) die der Einleitung des Verfahrens zugrunde liegenden Delikte.

Den Verfahren lagen 119 Delikte der Kategorie Raub/ Räuberische Erpressung zugrunde (27 Prozent der Fälle). Abbildung 26 zeigt, dass es sich dabei vor allem um Raub (44 Prozent der Fälle[425], 52 Nennungen), räuberische Erpressung (34 Prozent der Fälle, 40 Nennungen) und um schweren Raub (22 Prozent der Fälle, 26 Nennungen) handelte. Überwiegend (67 Prozent) konnten diese Delikte als Straßenraub näher spezifiziert werden (62 Nennungen).

Die Schadenshöhe lag zwischen zehn und 213 000 Euro (Mean: 4 815; Median: 240). In etwa 70 Prozent der Fälle blieb die Schadenshöhe unter 500 Euro. Damit ist die Schadenshöhe durchaus vergleichbar mit dem in der polizeilichen Kriminalstatistik nachgewiesenen durchschnittlichen Schadensaufkommen bei Raub- und Erpressungsdelikten[426].

Die Beschuldigten, die eines Raubes oder einer räuberischen Erpressung verdächtigt wurden, waren überwiegend erwachsen. 62 Prozent der Beschuldigten waren über 21 Jahre alt. Bei gesonderter Betrachtung der Straßenraubfälle, in denen dem Opfer z. B. seine Tasche samt Mobiltelefon entrissen wird, verändert sich das Bild sehr deutlich. Fast zwei Drittel der Beschuldigten (20), die solcher Mobiltelefonraubfälle verdächtig sind, sind unter 21 Jahre alt (siehe Abbildung 27). Es handelt sich bei diesen Fällen demnach um die gewöhnlich als „Abzocke unter Jugendlichen“ bezeichneten Raubfälle. Zu berücksichtigen ist, dass bei den Straßenraubfällen der Täter – trotz des Zugriffs auf die Verkehrsdaten – in 39 Fällen unbekannt geblieben ist.

[425] Es waren Mehrfachnennungen möglich.

[426] Bundeskriminalamt, Polizeiliche Kriminalstatistik 2005, Wiesbaden 2006, S. 147.

Abbildung 25

Ermittlungsdelikte in den Verfahren

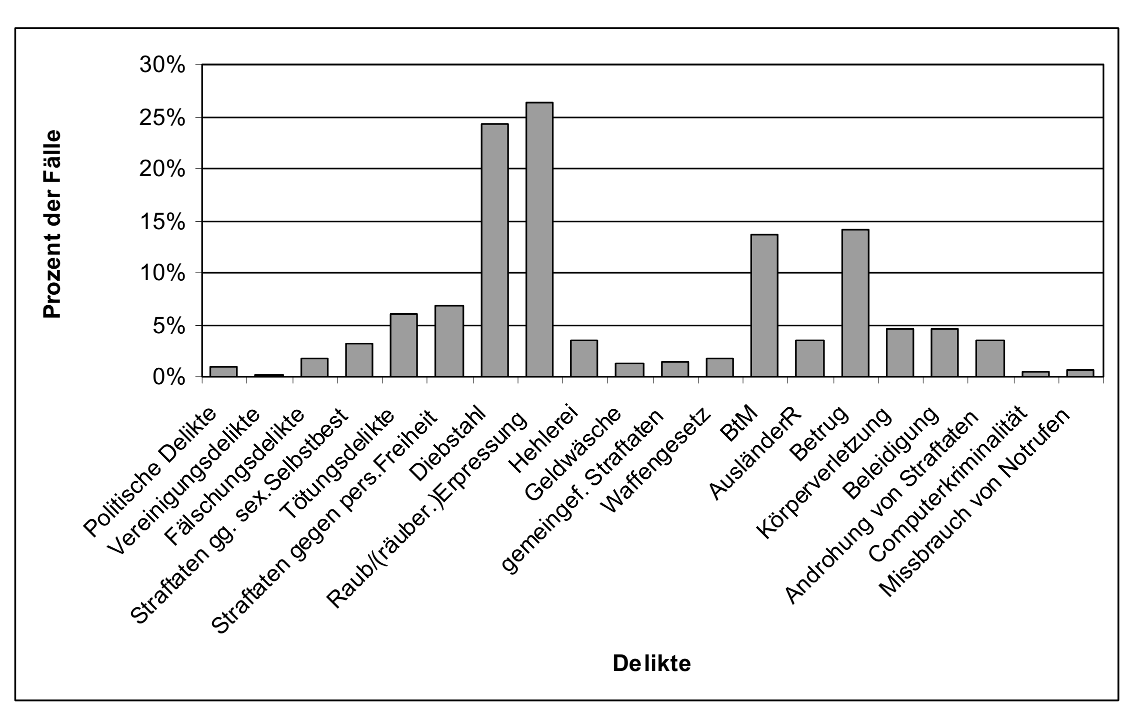


Abbildung 26



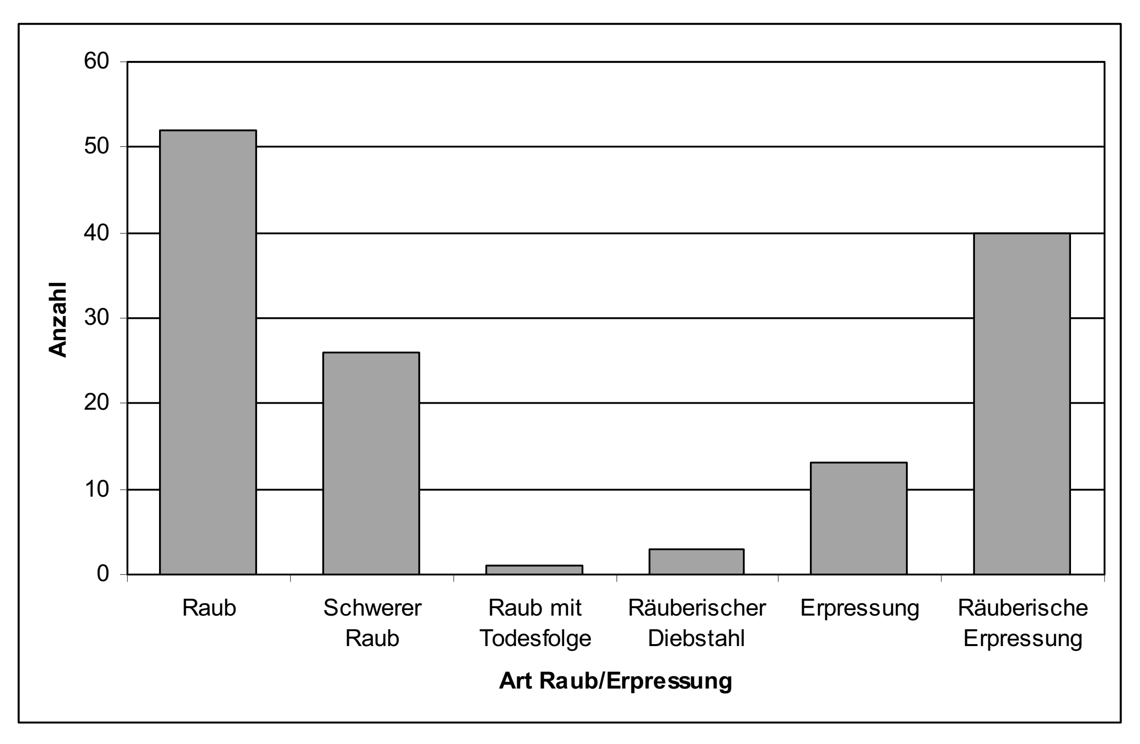
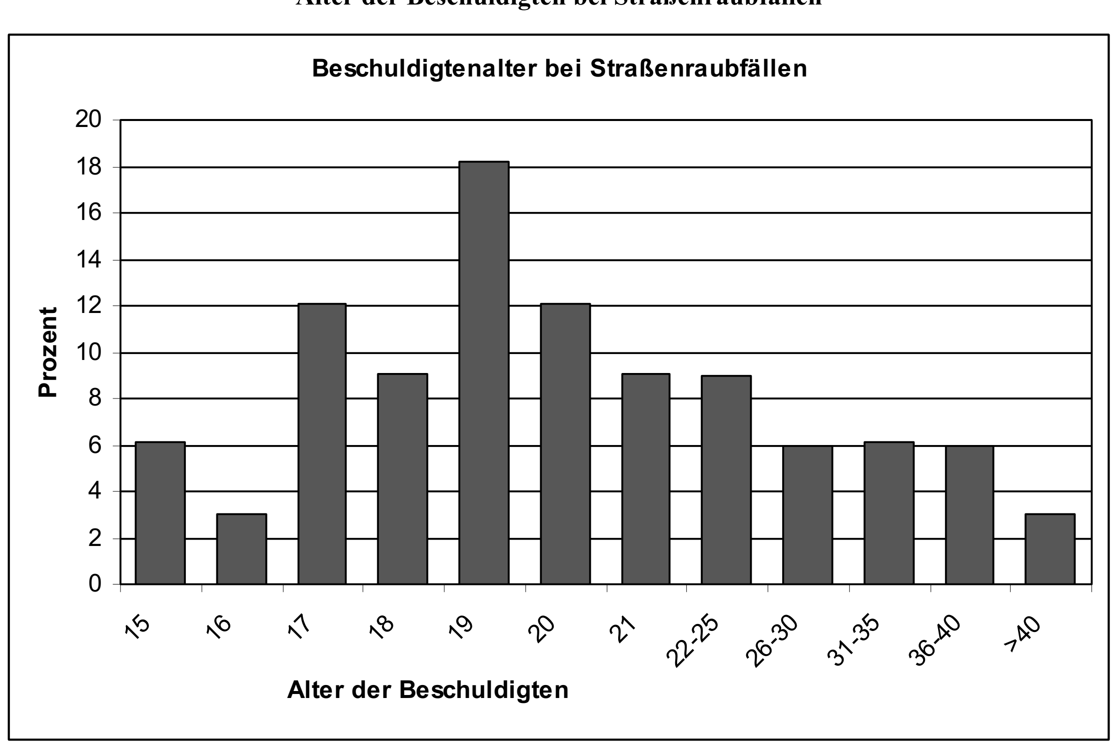


Abbildung 27

Alter der Beschuldigten bei Straßenraubfällen



Wie in Abbildung 28 dargestellt, handelt es sich bei den den Verfahren zugrundeliegenden Diebstählen überwiegend um besonders schwere Fälle des Diebstahls (§ 243 StGB; 56 Prozent der Fälle, N = 61). Der einfache Diebstahl gab in 18 Prozent der Fälle (N = 20) Anlass für das Verfahren.

Vom Erscheinungsbild her handelte es sich oftmals um Einbruchsdiebstähle (46), Kfz-Diebstähle (15) und um die Entwendung von Sachen aus aufgebrochenen Kraftfahrzeugen (12). Die Schadenshöhe variierte zwischen 41 Euro und 250 000 Euro (Mittelwert: 15 944; Median: 2 300).

Den 467 Verfahren lagen 27 Tötungsdelikte (6 Prozent der Fälle) zugrunde. Dabei handelte es sich in 17 Fällen um Mord und in sieben um Totschlag; in drei Fällen konnte nicht näher spezifiziert werden, um welche Art von Tötungsdelikt es sich handelt. Meist war in diesen Fällen nur ein Opfer betroffen.

Mit den ausgewerteten Verfahren wurden in 15 Prozent der Fälle Betrugsdelikte verfolgt. Am häufigsten war dabei der sog. Enkeltrick (53 Prozent dieser Fälle). Die Schadenshöhe variierte zwischen 423 Euro und 1 727 178 Euro (Mittelwert: 57 316; Median: 4 700).

Bei den Straftaten gegen die persönliche Freiheit, die den Verfahren zugrunde liegen, handelt es sich überwiegend um Bedrohungen (§ 241 StGB; 16 Nennungen, 52 Prozent). Abbildung 29 lässt sich entnehmen, dass Menschenhandel zu Zwecken der sexuellen Ausbeutung (§§ 181a ff. a. F., heute § 232 StGB) sowie erpresserischer Menschenraub (§ 239a StGB) etwas häufiger waren als Freiheitsberaubung (§ 239 StGB), Nötigung (§ 240 StGB) und die Entziehung Minderjähriger (§ 235 StGB).

Da Telekommunikationsüberwachungsmaßnahmen häufig mit Organisierter Kriminalität in Verbindung gebracht werden, wurden entsprechende Fälle anhand der Akteninformationen identifiziert. Nach der Definition der Arbeitsgruppe Justiz und Polizei von 1990[427] ist Organisierte Kriminalität „die von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen oder unter Anwendung von Gewalt oder anderer zur Einschüchterung

[427] RiStBV Anlage E, Punkt 2.1.

Abbildung 28

Art der Diebstahlsdelikte

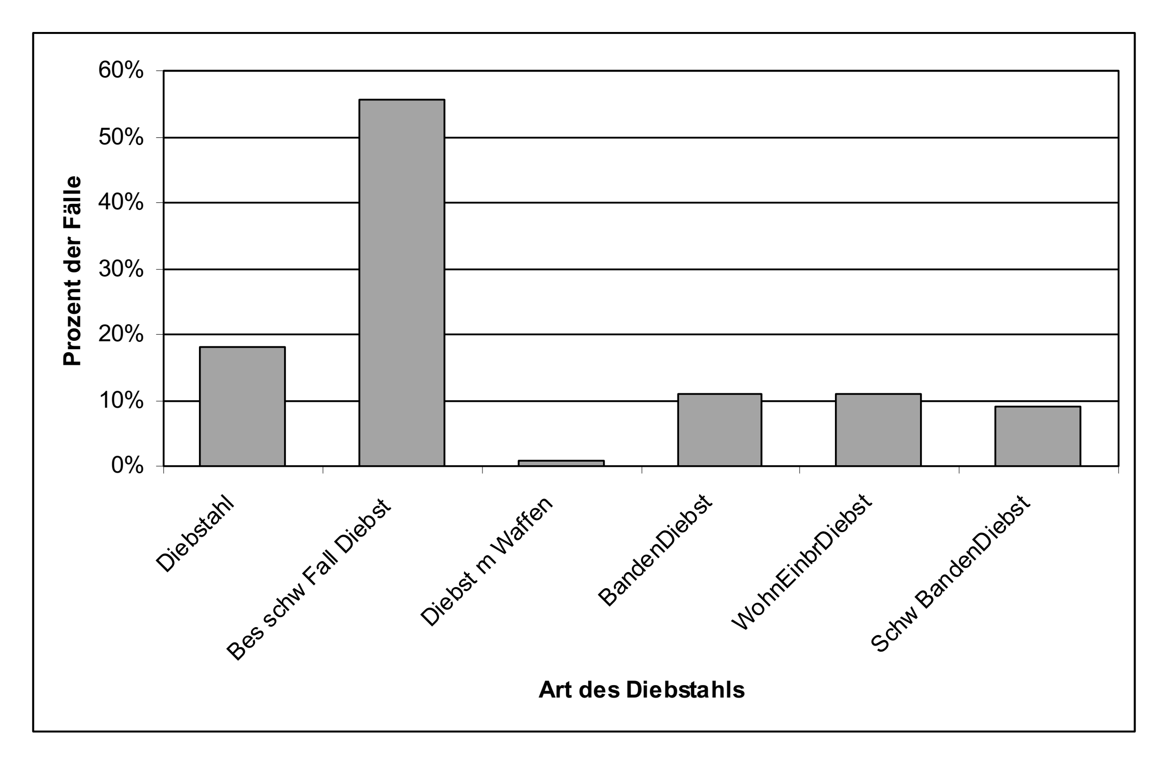
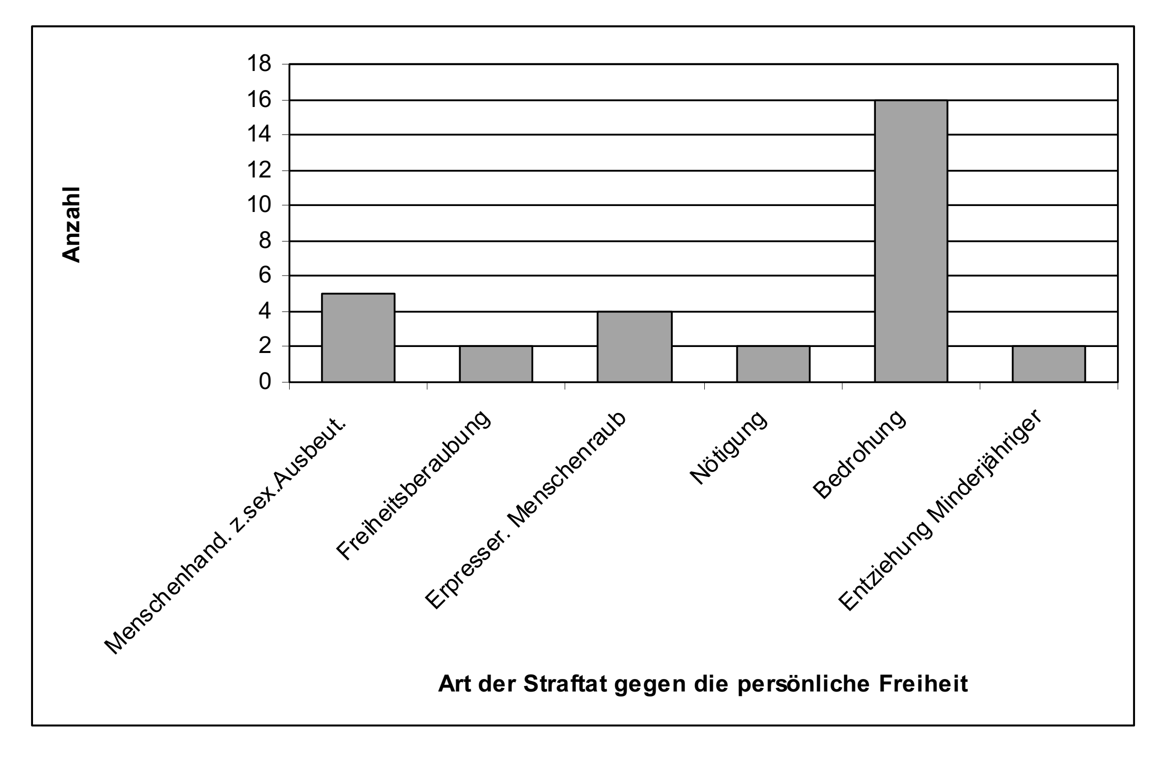


Abbildung 29



Art der Delikte gegen die persönliche Freiheit



geeigneter Mittel oder unter Einflussnahme von Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken“. Dieser Definition wurden neun Elemente entnommen, deren Auftreten in den Verfahrensakten erhoben wurde: Gewinnstreben, planmäßige Begehung, Erheblichkeit der Straftaten, mehr als zwei Beteiligte, längere Dauer, Arbeitsteilung, gewerbliche Strukturen, Gewaltanwendung und Einfluss von Politik und Medien. In 85 der ausgewerteten Verfahren fanden sich Hinweise auf Elemente der Organisierten Kriminalität. Dabei wurden in 64 Verfahren mindestens drei Elemente Organisierter Kriminalität festgestellt. Das Vorliegen von vier und fünf Elementen wurde für je 13 Verfahren und sechs Elemente bei 14 Verfahren beobachtet.

Schon die allgemeinen Verteilungen der die Ermittlungsverfahren begründenden Straftatbestände sprechen demnach dafür, dass sich die Verkehrsdatenabfrage auf ein weites Deliktsspektrum bezieht, dass also nicht der Telekommunikationsüberwachung entsprechende Konzentrationen bei Transaktionsdelikten (insbesondere Betäubungsmittelstraftaten) beobachtet werden können, und dass von daher die Verkehrsdatenabfrage von der Phänomenologie der Delikte her gesehen als weit greifendes Ermittlungsinstrument angesehen werden kann. Dies deckt sich im Kern mit den Befunden aus der Untersuchung des Bundeskriminalamts aus dem Jahr 2005.[428]

II. Schriftliche Befragung

1. Häufigkeit der Anordnungen

Im Durchschnitt wurden von den Befragten für das Jahr 2005 eine Zahl von 15 Verfahren mit Anordnungen von Verkehrsdatenabfragen angegeben (Median: 6)[429]. Allerdings gaben 20 Prozent der Befragten an, dass sie bislang nicht an Verfahren mit Maßnahmen nach §§ 100g, 100h StPO beteiligt waren.

Differenziert nach Dezernaten ergeben sich signifikante Unterschiede in der Anzahl der Verfahren im Jahr 2005. Dies erklärt sich zum Teil aus deliktsspezifischen Gründen. So sind die Verfahrenszahlen in Dezernaten wie Verkehrstrafsachen oder auch sonstigen Straftaten gering. Höhere Zahlen sind in den Dezernaten Betäubungsmittelsachen, Sexualdelikte sowie Computer- und Internetstrafsachen zu verzeichnen.

---

[428] *Mahnken*, 2005.

[429] Bei dieser Berechnung wurden die dreifach erwähnten Extremwerte von 1 000 Anordnungen pro Jahr weggelassen.

Unterschiede sind auch entlang der Bundesländer festzustellen, die sich nicht allein durch die Unterschiede zwischen Stadt- und Landstaaten erklären lassen. Eine gewisse Differenz ergibt sich im Vergleich von West- und Ostdeutschland. In Ostdeutschland werden nur etwa halb so viele Verfahren im Jahr 2005 angegeben wie in Westdeutschland.[430]

2. Geschätzte Anzahl von Anträgen und Anordnungen

Fragen zu Schätzungen über die Häufigkeit der Anträge und Anordnungen im Jahr 2005 wurden für die Staatsanwälte selbst, die Abteilung und die gesamte Behörde gestellt. Dabei ist selbstverständlich zu berücksichtigen, dass viele Befragte darauf hinwiesen, dass eine sichere Schätzung aufgrund der fehlenden Statistik kaum möglich und die Einschätzung für die Abteilung bzw. für die gesamte Behörde eher spekulativ sei. Dabei geht es hier nicht allein um Angaben zu den tatsächlich durchgeführten Maßnahmen. Vielmehr sollen durch Schätzungen Anhaltspunkte für die Beantwortung der Frage generiert werden, ob aus einer quantitativen Perspektive die Verkehrsdatenabfrage ein berufliches Alltagsereignis ist.

Wie sich aus Tabelle 13[431] ergibt, steigt die geschätzte Anzahl von Anträgen und Anordnungen nach §§ 100g, 100h StPO erwartungsgemäß von der individuellen Erfahrung über die Einschätzung der jeweiligen Abteilung bis zur Wahrnehmung der Praxis in der Behörde insgesamt. Im Mittel werden nach der eigenen Erfahrung 23, in der Abteilung 88 und in der Behörde 558 Anträge gestellt. Die Schätzungen für die tatsächlichen Anordnungen liegen etwa 10 Prozent unter den Schätzungen für die Anträge. Die Befragten gehen demnach davon aus, dass die Anträge zu etwa 10 Prozent abgelehnt werden. Hier steigt die Anzahl der Anordnungen von 21 (Eigenerfahrung) über 79 (Abteilung) auf 498 (gesamte Behörde).

[430] Auch lassen sich die Unterschiede entlang der Länder nicht durch unterschiedliche Dezernatsverteilungen in den Ländern erklären. Die unterschiedliche Anzahl der Verfahren kann zu 7 Prozent durch die Länder und zu 4 Prozent durch die Art des Dezernats erklärt werden. Zusammen betrachtet werden 11 Prozent der Varianz erklärt. (R^2 der entsprechenden Regressionen).

[431] Unter Nennungen (N) ist dabei die Anzahl der Befragten zu verstehen, die diese Frage beantwortet haben.

Die Veränderungen hinsichtlich der Anzahl der Anträge bezüglich des Vorjahres schätzten 65 Prozent mit gleich bleibend ein, während 32 Prozent von einer Steigerung berichteten. Bei den tatsächlichen Anordnungen wurde von 21 Prozent der Befragten ein Anstieg wahrgenommen, während 78 Prozent die Anzahl der Anordnungen als gleichbleibend beschrieb.

Die Schätzungen hinsichtlich der Anwendungsbereiche der Verkehrsdatenabfrage zeigen, dass überwiegend vorhandene Verkehrsdaten abgerufen werden (ca. 70 Prozent, siehe Tabelle 14). Dies deckt sich recht gut mit den aus der Aktenuntersuchung bekannten Verteilungen. Zukünftige Verkehrsdaten werden nach der Einschätzung der Befragten zu ca. 20 Prozent abgefragt und die Zielwahlsuche zu ca. 10 Prozent durchgeführt. Bei den Schätzungen gibt es keine Unterschiede zwischen Anträgen und Anordnungen. Leichte Veränderungen sind von den Schätzungen für die eigene Erfahrung bis zu denen für die gesamte Behörde insofern festzustellen, als der Anteil für vorhandene Verkehrsdaten für die Behörde etwas an Umfang verliert und dafür die Anteile für die komplexeren Maßnahmen (zukünftige Verkehrsdaten und Zielwahlsuche) etwas ansteigen.

Aus Tabelle 15 ergibt sich, dass nach Einschätzung der Befragten bei der kombinierten Anwendung der einzelnen Anwendungsbereiche der Verkehrsdatenabfrage, vor allem die Abfrage von vorhandenen und zukünftigen Verkehrsdaten zusammen angeordnet wird. Dabei nimmt der Umfang der geschätzten Anordnungen von der Eigenerfahrung bis hin zur gesamten Behörde leicht ab (von 66 Prozent auf 60 Prozent). Am zweithäufigsten ist nach Angabe der Befragten die kombinierte Anwendung der Abfrage vorhandener Verkehrsdaten und der Zielwahlsuche, wobei es keine Unterschiede zwischen den Schätzungen aufgrund den eigenen Erfahrungen, für die Abteilung und die gesamte Behörde gibt (18 bzw. 19 Prozent). In geringerem Umfang werden die Abfrage zukünftiger Verkehrsdaten zusammen mit der Zielwahlsuche und die Kombination aller drei genannter Anwendungsbereiche angeordnet (beide ca. 9 Prozent). Dabei ist eine leichte Steigerung des geschätzten Umfangs dieser kombinierten Anwendungen von der Eigenerfahrung hin zur gesamten Behörde zu bemerken (von 7 Prozent auf 11 Prozent bzw. von 8 Prozent auf 11 Prozent).

Tabelle 13

Geschätzte Anzahl der Anträge und Anordnungen im Jahr 2005

	Eigenerfahrung			Abteilung			Behörde		
	N	Mittelw.	Median	N	Mittelw.	Median	N	Mittelw.	Median
Anträge	580	23,2	10	412	88,0	50	329	557,6	200
Anordnungen	560	20,5	10	381	78,5	40	312	497,7	180

Tabelle 14

Geschätzte Anzahl von Anträgen und Anordnungen unterteilt nach Anwendungsbereichen*

Angaben in %	Eigenerfahrung		Abteilung		Behörde	
	Anträge	Anordnungen	Anträge	Anordnungen	Anträge	Anordnungen
vorhandene VD	*71*	*71*	*70*	*70*	*65*	*64*
zukünftige VD	*18*	*18*	*20*	*20*	*22*	*23*
Zielwahlsuche	*11*	*11*	*10*	*10*	*13*	*13*

* VD = Verkehrsdaten.

Tabelle 15

Geschätzte Anzahl an Anordnungen bei kombinierten Anwendungsbereichen*

Angaben in %	Eigenerfahrung	Abteilung	Behörde
vorhandene mit zukünftigen VD	*66*	*62*	*60*
vorhandene VD mit ZWS	*18*	*18*	*19*
zukünftige VD mit ZWS	*7*	*9*	*11*
vorhandene VD, zukünftige VD und ZWS	*8*	*9*	*11*

* VD = Verkehrsdaten, ZWS = Zielwahlsuche.

III. Experteninterviews

Die Ergebnisse der Experteninterviews stützen sich auf Gespräche mit 53 Personen. Dabei handelt es sich um zehn (Ermittlungs-)Richter, 13 Staatsanwälte, 16 Polizeibeamte, vier Strafverteidiger, sechs Telekommunikationsanbieter und vier Datenschutzbeauftragte. Die Befragten arbeiten in den Bundesländern Baden-Württemberg, Berlin, Mecklenburg-Vorpommern und Nordrhein-Westfalen. Aus Anonymisierungsgründen werden die genauen Orte nicht angegeben. Der Inhalt der Gespräche wird zusammenfassend wiedergegeben.

C. Anordnungspraxis und Durchführung der Maßnahme

I. Delikte und Verdachtsgrad

1. Schriftliche Befragung

a) Delikte

Die Befragten gaben an, dass sie im Jahr 2005 im Durchschnitt 142 Anträge nach §§ 100g, 100h StPO gestellt haben, denen solche Straftaten zugrunde lagen, die in Tabelle 16 aufgeführt sind (Katalogstraftaten i. S. v. § 100a Satz 1 StPO und sonstige Straftaten, die *nicht* mittels Endeinrichtung begangen wurden). Der Straftatenkatalog des § 100a Satz 1 StPO, auf den § 100g I Satz 1 StPO verweist, umfasst nur bestimmte Ausprägungen der jeweiligen Deliktsgruppen. So ist beispielsweise der Bandendiebstahl erfasst, nicht aber der einfache Diebstahl. Aus Gründen der Übersichtlichkeit wurden als Antwortmöglichkeiten jedoch die Deliktsgruppen insgesamt (Diebstahl) aufgeführt.

In Tabelle 16 wird angegeben, wie häufig bestimmte Delikte genannt wurden (z. B. wurden politische Delikte 22-mal erwähnt) und welcher Prozentsatz der Befragten diese Delikte genannt hat. Da die Befragten mehrere Delikte nennen konnten, summieren sich diese Prozentsätze über 100 Prozent. Im Schnitt nannten die Befragten 2,6 Delikte. Weiter ist aufgeführt, wie viele Anträge auf Anordnung einer Maßnahme nach §§ 100g, 100h StPO, denen dieses Delikt zugrunde lag, die Befragten im Jahr 2005 insgesamt gestellt haben und wie sich diese Anträge auf die genannten Delikte verteilen.

Am häufigsten wurden als den Anträgen zugrundeliegende Delikte (in dieser Deliktsgruppe) Raub bzw. räuberische Erpressung (39,3 Prozent) und Diebstahl (37,4 Prozent) von den Befragten genannt. Ebenfalls sehr häufig wurden Betrug (26,6 Prozent) und Betäubungsmitteldelikte (25,6 Prozent) aufgeführt. Etwas weniger häufig lagen nach Angaben der Befragten den Anträgen Tötungsdelikte (14,4 Prozent), Erpressung (12,2 Prozent), Hehlerei (10,7 Prozent) und Menschenhandel (9,9 Prozent) zugrunde. Verstöße gegen das Ausländerrecht (8,6 Prozent der Nennungen), Sexualdelikte (7,6 Prozent), Verbreitung pornographischer Schriften (7,1 Prozent), sexueller Missbrauch von Kindern (6 Prozent) und Körperverletzung (6 Prozent) waren etwas seltener. Auch gemeingefährliche Straftaten (5,6 Prozent), Fälschungsdelikte (5,1 Pro-

Tabelle 16

Katalogdelikte und nicht mittels Endeinrichtung begangene Delikte

Deliktskategorien	Anzahl Nennungen	Häufigkeit Nennung	Anzahl gestellter § 100gh-Anträge	Verteilung der gestellten Anträge auf die Delikte
Politische Delikte	22	*3,6 %*	102	*1,0 %*
Vereinigungsdelikte	20	*3,3 %*	54	*0,5 %*
Fälschungsdelikte	31	*5,1 %*	167	*1,7 %*
Sex. Missbrauch von Kindern	36	*6,0 %*	113	*1,1 %*
Verbreit. pornograph. Schriften	43	*7,1 %*	386	*3,8 %*
Tötungsdelikte	87	*14,4 %*	285	*2,8 %*
Menschenhandel, Geiselnahme	60	*9,9 %*	137	*1,4 %*
Diebstahl	226	*37,4 %*	1 635	*16,2 %*
Raub/Räuberische Erpressung	238	*39,3 %*	1 201	*11,9 %*
Erpressung	74	*12,2 %*	262	*2,6 %*
Hehlerei	65	*10,7 %*	260	*2,6 %*
Geldwäsche	22	*3,6 %*	140	*1,4 %*
Gemeingefährl. Straftaten	34	*5,6 %*	96	*1,0 %*
Verstöße gg. Waffengesetz	30	*5,0 %*	68	*0,7 %*
Verst. gg. Außenwirtschaftsgesetz	6	*1,0 %*	2	*0,0 %*
Betäubungsmitteldelikte	155	*25,6 %*	2 147	*21,3 %*
Verst. gg. Ausländerrecht	52	*8,6 %*	304	*3,0 %*
Betrug	161	*26,6 %*	1 680	*16,6 %*
Sex. Missbr./Nötigung/Vergewalt.	46	*7,6 %*	160	*1,6 %*
Androhung. v. Straftat	29	*4,8 %*	105	*1,0 %*
Körperverletzung	36	*6,0 %*	84	*0,8 %*
Nötigung	24	*4,0 %*	26	*0,3 %*
Entziehung Minderjähriger	9	*1,5 %*	5	*0,0 %*
Sonstige	58	*9,6 %*	673	*6,7 %*
Insgesamt	**1 564**	***258,5 %***	**10 092**	***100 %***

Anmerkung: Delikte, die eindeutig nicht unter den Katalog des § 100a StPO fallen, sind hervorgehoben.

zent), Verstöße gegen das Waffengesetz (5 Prozent), Androhung von Straftaten (4,8 Prozent) sowie Nötigung (4 Prozent) wurden von den Befragten seltener genannt. Nach den Angaben der Befragten lagen im Jahr 2005 den Anträgen nur in Ausnahmefällen politische Delikte, Vereinigungsdelikte, Geldwäsche, Verstöße gegen das Außenwirtschaftsgesetz sowie die Entziehung Minderjähriger zugrunde. Die Verteilungen in den Antworten der Staatsanwälte decken sich recht gut mit den Deliktsverteilungen, die für die Aktenuntersuchung bereits vorgestellt wurden.

Zusätzlich zu den 10 092 erwähnten Anträgen nach §§ 100g, 100h StPO mit zugrunde liegenden Straftaten von (erheblicher) Bedeutung werden noch 5 903 Anträge in Verfahren, in denen Straftaten, die mittels Endeinrichtung begangen wurden, genannt. Im Detail verteilen sich diese entsprechend der Tabelle 17.

Tabelle 17

Straftaten mittels Endeinrichtung

Deliktskategorien	**Anzahl Nennungen**	**Häufigkeit Nennung**	**Summe der 100gh-Anträge**	**Verteilung der Anträge auf die Delikte**
Beleidigung per Telefon etc.	199	*48,7%*	534	*9,0%*
Bedrohung per Telefon etc.	175	*42,8%*	416	*7,0%*
Telefonterror / Massen-E-Mails	38	*9,3%*	68	*1,2%*
Sex. belästigende Anrufe etc.	83	*20,3%*	225	*3,8%*
Verbr. porno./rechtsrad. Schriften per PC	57	*13,9%*	464	*7,9%*
Computerbetrug	146	*35,7%*	1 913	*32,4%*
Datenveränderung, Computer-sabotage	52	*12,7%*	279	*4,7%*
Datenfälschung	28	*6,8%*	169	*2,9%*
Ausspähen von Daten	54	*13,2%*	266	*4,5%*
Missbrauch von Notrufen	56	*13,7%*	137	*2,3%*
Warenbestellbetrug	95	*23,2%*	675	*11,4%*
Urheberrechtsverletzungen	49	*12,0%*	509	*8,6%*
Enkeltrick	12	*2,9%*	34	*0,6%*
Sonstige	42	*10,3%*	216	*3,7%*
	1 086	***265,5%***	**5 903**	***100,0%***

Am häufigsten wurden Beleidigung per Telefon oder mittels sonstiger Endeinrichtung (49 Prozent) sowie Bedrohung mittels Endeinrichtung (43 Prozent) genannt. Auch Computerbetrug (36 Prozent), Warenbestellbetrug (23 Prozent) und sexuell belästigende Anrufe (20 Prozent) gehören zu den am häufigsten genannten Antworten. Weniger häufig gaben die Befragten die Verbreitung pornographischer oder rechtsradikaler Bilder und Schriften über Computer (14 Prozent), den Missbrauch von Notrufen (14 Prozent), das Ausspähen von Daten (13 Prozent), Datenveränderung (13 Prozent) sowie Urheberrechtsverletzungen (12 Prozent) an. Telefonterror (9 Prozent), Datenfälschung (7 Prozent) und der Enkeltrick (3 Prozent) waren die am seltensten genannten Antworten.

Sonstige Delikte, die von den Befragten aufgeführt wurden, betreffen Verstöße gegen das AuslG bzw. AufenthG, sonstiger Betrug und allgemein Betrug mittels Endeinrichtung, Steuerhinterziehung, Bestechung, Wohnungseinbruchsdiebstahl, Brandstiftung, Bildung einer kriminellen Vereinigung, Verstöße gegen das MarkenG und das Vortäuschen einer Straftat.

In Tabelle 18 werden die von den Befragten festgestellten Veränderungen der Häufigkeiten der verschiedenen Delikte im Vergleich zwischen 2004 und 2005 dargestellt.

Die Frage nach der Veränderung von Deliktshäufigkeiten wurde nur von 10 bis 20 Prozent der Befragten beantwortet. Ein Mittelwert von 1,5 entspricht dabei einer Tendenz genau zwischen gleich bleibend und steigend, ein Wert von 2 besagt keine Veränderung und 1 eine steigende Häufigkeit der Delikte. Zu fast gleichen Teilen wurden insbesondere bei Delikten, die mittels Computer begangen werden, steigende und gleich bleibende Tendenzen genannt, z. B. Computerbetrug, Urheberrechtsverletzungen, Verbreitung pornographischer/rechtsradikaler Schriften mittels Computer. Bei anderen Delikten wurden Steigerungen seltener angegeben.

Tabelle 18

Veränderungen im Auftreten der Häufigkeit verschiedener Delikte

Delikt	Nennungen	Mittelwert Tendenzen
Computerbetrug	141	*1,46*
Urheberrechtsverletzungen	62	*1,50*
Verbr. porn./rechtsrad. Bilder/Schriften per PC	73	*1,58*
Ausspähen von Daten	61	*1,61*
Telefonterror/Massen-E-Mails	55	*1,62*
Datenveränderung, Computersabotage	60	*1,62*
Warenbestellbetrug	97	*1,62*
Sex. belästigende Anrufe, E-Mails, SMS	91	*1,64*
Betrug	156	*1,65*
Datenfälschung	45	*1,69*
Verbreit. pornogr. Schriften	68	*1,71*
Betäubungsmitteldelikte	168	*1,71*
Diebstahl	221	*1,72*
Beleidigung mittels Endeinr.	186	*1,73*
Sex. Missbrauch/Nötigung, Vergewaltigung	66	*1,76*
Bedrohung mittels Endeinr.	161	*1,78*
Raub/Räuberische Erpressung	225	*1,80*
Gemeingefährliche Straftaten	54	*1,81*
Hehlerei	76	*1,82*
Erpressung	84	*1,83*
Enkeltrick	19	*1,84*
Fälschungsdelikte	47	*1,85*
Menschenhandel, Geiselnahme	79	*1,86*
Sonstige	69	*1,86*
Tötungsdelikte	109	*1,87*
Körperverletzung	61	*1,87*
Geldwäsche	43	*1,88*
Verstöße gg. Waffengesetz	56	*1,88*
Politische Delikte	44	*1,89*
Sex.Missbrauch v. Kindern	59	*1,90*
Nötigung	44	*1,91*
Verst. gg. Ausländerrecht	78	*1,92*
Vereinigungsdelikte	41	*1,93*
Androhung von Straftaten	50	*1,94*
Entziehung Minderjähriger	31	*1,94*
Verst. gg. Außenwirtschaftsgesetz	25	*2,00*
Missbrauch von Notrufen	68	*2,00*

b) Straftat von erheblicher Bedeutung

60 Prozent der Befragten halten keine Änderung von § 100g I Satz 1 StPO in Bezug auf die Formulierung „Straftat von erheblicher Bedeutung, insbesondere einer der in § 100a Satz 1 StPO genannten Straftaten“ für notwendig. Von den Befragten (40 Prozent), die eine Änderung für erforderlich erachten, waren 11 Prozent für eine Beschränkung auf Katalogstraftaten i. S. v. § 100a StPO und eine Streichung des Begriffs der Straftat von erheblicher Bedeutung. Demgegenüber plädierten 68 Prozent für die Beschränkung auf den Begriff der Straftat von erheblicher Bedeutung ohne Verweis auf § 100a StPO. 21 Prozent der Befragten schlugen weitere Änderungen vor[432]. Von diesen waren 47 Prozent (ca. 10 Prozent aller Befragten) für eine Ausdehnung auf alle Straftaten. 20 Prozent (ca. 4 Prozent aller Befragten) befürworten eine Erweiterung des Straftatenkatalogs des § 100a StPO auf andere Straftaten, wie beispielsweise den gewerbsmäßigen Betrug. Weitere 11 Prozent wünschen sich allgemein eine eindeutigere, konkretere Regelung. 7,6 Prozent sprechen sich für eine Streichung des Begriffs der Straftat von erheblicher Bedeutung und des Verweises auf den Katalog des § 100a StPO aus und meinen, dass eine Verhältnismäßigkeitsprüfung genüge. Jeweils 4,5 Prozent würden die Formulierung „Straftat von nicht unerheblicher Bedeutung“ sowie lediglich den Ausschluss geringfügiger Taten bevorzugen. Weitere 4,5 Prozent befürworten einen eigenen Straftatenkatalog für die Verkehrsdatenabfrage.

Auf die Frage, ob es sich bei der Straftatbegehung mittels Endeinrichtung ebenfalls um eine *erhebliche* Straftat sollte handeln müssen, damit eine Verkehrsdatenabfrage durchgeführt werden kann, antworteten die Befragten überwiegend mit „nein“ (75 Prozent). Die Minderheit (25 Prozent) bejahte die Frage. Zur Begründung für die Voraussetzung einer Straftat von erheblicher Bedeutung wurde angeführt, dass ein erheblicher Eingriff in Grundrechte vorliege (33 Prozent der Befragten, die mit ja antworteten). Weitere 23 Prozent geben an, dass sich dies aus dem Wortlaut des § 100g I Satz 1 StPO ergebe. Für 10 Prozent dieser Befragten ergibt sich diese Voraussetzung aus der Gesetzessystematik. Andere gaben an, dass der Grundsatz der Verhältnismäßigkeit gewahrt werden müsse (9 Prozent) und sonst die Gefahr einer Ausuferung der Anwendung der Maßnahme bestehe (10 Prozent). 6 Prozent waren der Ansicht, dass eine gleichförmige Handhabung der Maßnahme, d. h. eine gleiche Anwendung der beiden Alternativen, gewährleistet sein müsse.

Diejenigen mit Nein-Antworten führten als Begründung dazu aus, dass sich dies eindeutig aus dem Wortlaut der Norm ergebe (34 Prozent der Befragten, die mit nein antworteten). Weitere 19 Prozent stellten auf das Wort „oder“ im Gesetzestext ab. Weitere 20 Prozent gaben an, dass eine Aufklärung von Straftaten, die mittels Endeinrichtung begangen wurden, sonst unmöglich oder zumindest erschwert wäre. Jeweils 9 Prozent stellten zur Begründung darauf ab, dass die Begriffe „Straftat von erheblicher Bedeutung“ und „mittels Endeinrichtung begangene Straftat“ erkennbar alternativ gebraucht würden und dass letztere sonst keine selbständige Bedeutung habe und daher überflüssig sei. 5 Prozent gaben an, dass die Verkehrsdatenabfrage oft die einzige Möglichkeit zur Aufklärung mittels Endeinrichtung begangener Straftaten sei. Zudem wurde angeführt, dass die Endeinrichtung als Tatmittel benutzt werde und der Täter deshalb weniger schutzbedürftig sei (8 Prozent). Weitere Begründungen waren opferschutzbezogen, nämlich dass der Geschädigte sonst nahezu schutzlos gestellt wäre und daher auch mindere Kriminalität erfasst sein soll.

c) Verdachtsgrad

90 Prozent der Befragten (731) halten den gesetzlich festgelegten Verdachtsgrad für angemessen. Als Begründung wurde angeführt, dass die Verkehrsdatenabfrage einen erheblichen Eingriff in Grundrechte darstelle und der Verdachtsgrad zum Grundrechtsschutz erforderlich sei (91 Befragte, 25 Prozent dieser Gruppe[433]). Dagegen sahen zehn Befragte die Eingriffsintensität als relativ gering und den festgelegten Verdachtsgrad dafür als ausreichend an. Als weitere Begründung für die Angemessenheit des Verdachtsgrads wurde angeführt, dass so die Verhältnismäßigkeit gewahrt werde, d. h. ein ausgewogenes Verhältnis zwischen dem Schutz des Betroffenen und dem Strafverfolgungsinteresse möglich sei (53 Befragte, 14 Prozent dieser Gruppe). 21-mal wurde genannt, dass die Anwendung der Maßnahme ansonsten ausufern würde. Mehrfach wurde ganz allgemein begründet, dass der geregelte Verdachtsgrad, d. h. der einfache Tatverdacht, ausreichend sei (42 Befragte). Weitere Begründungen waren, dass damit eine adäquate Eingriffsschwelle geschaffen werde, dass bloße Vermutungen nicht ausreichten und eine objektivierbare Verdachtslage gegeben sein müsse. Zudem wurde angegeben, dass die Maßnahme sonst zur Ausforschung benutzt werden könne. Auf der anderen Seite wurde ausgeführt, dass durch einen höheren Verdachtsgrad die Ermittlungen zu sehr erschwert würden und die Ermittlungsmaßnahme nicht praktikabel wäre. Zudem stünde die Verkehrsdatenabfrage oft am Anfang der Ermittlungen und ein höherer Verdachtsgrad sei meist noch nicht gegeben. Weiter wurde vereinzelt angeführt, dass die Regelung auch § 100a StPO sowie der Systematik der anderen Maßnahmen entspreche.

Diejenigen, die den Verdachtsgrad nicht für angemessen hielten (10 Prozent bzw. 84 Befragte), gaben u. a. als Begründung an, dass es sich um keinen erheblichen Grundrechtseingriff handle (zehn Befragte, 15 Prozent dieser Gruppe), der Eingriff weniger gravierend als z. B. bei der Durchsuchung sei und trotzdem der gleiche Maßstab gelte (zwölf Befragte). Andere stellten allgemein auf die zu hohen bzw. einschränkenden Anforderungen an den Verdachtsgrad ab (zehn Befragte). Man stehe bei der Erhebung der Daten oft noch beim Beginn der Ermittlungen

[432] In diesem Fall traten einige Mehrfachnennungen auf.

[433] Hier – wie auch bei den Nennungen der Begründungen in den folgenden Fragen – konnten mehrere Begründungen angegeben werden. Daher summieren sich die Prozente ggf. über 100 Prozent.

(sieben Befragte). Acht Befragte fanden den Verdachtsgrad zwar nicht zu streng, begründeten die Unangemessenheit des Verdachtsgrads aber mit dessen Unbestimmtheit.

Zusammenfassend kann man sagen, dass der Großteil der Befragten den festgelegten Verdachtsgrad für erforderlich, aber auch als ausreichend erachtet. Dabei gibt es keine Unterschiede entlang der Bundesländer und Dezernate.

2. Aktenanalyse

Insgesamt befanden sich in den 467 ausgewerteten Verfahren 1257 Beschlüsse nach §§ 100g, 100h StPO. Auch hier zeigt sich ein breites Spektrum an Anlassstraftaten. Dabei sind Straftaten von erheblicher Bedeutung und mittels Endeinrichtung begangene Straftaten zu unterscheiden. Wie bereits ausgeführt umfasst der Begriff der Straftat von erheblicher Bedeutung Straftaten, die der mittleren Kriminalität zuzuordnen sind. Zudem verweist § 100g I Satz 1 StPO auf den Straftatenkatalog des § 100a Satz 1 StPO. Zumindest diese Delikte sind also uneingeschränkt als Straftaten von erheblicher Bedeutung anzusehen.

70 Prozent der Beschlüsse liegen ausschließlich Katalogdelikte i. S. v. § 100a Satz 1 StPO zugrunde. In weiteren 2 Prozent der Beschlüsse ist neben einem Katalogdelikt auch eine andere Straftat erwähnt. Bei den restlichen 28 Prozent handelt es sich um Beschlüsse, bei denen ausschließlich andere Delikte Grundlage waren.

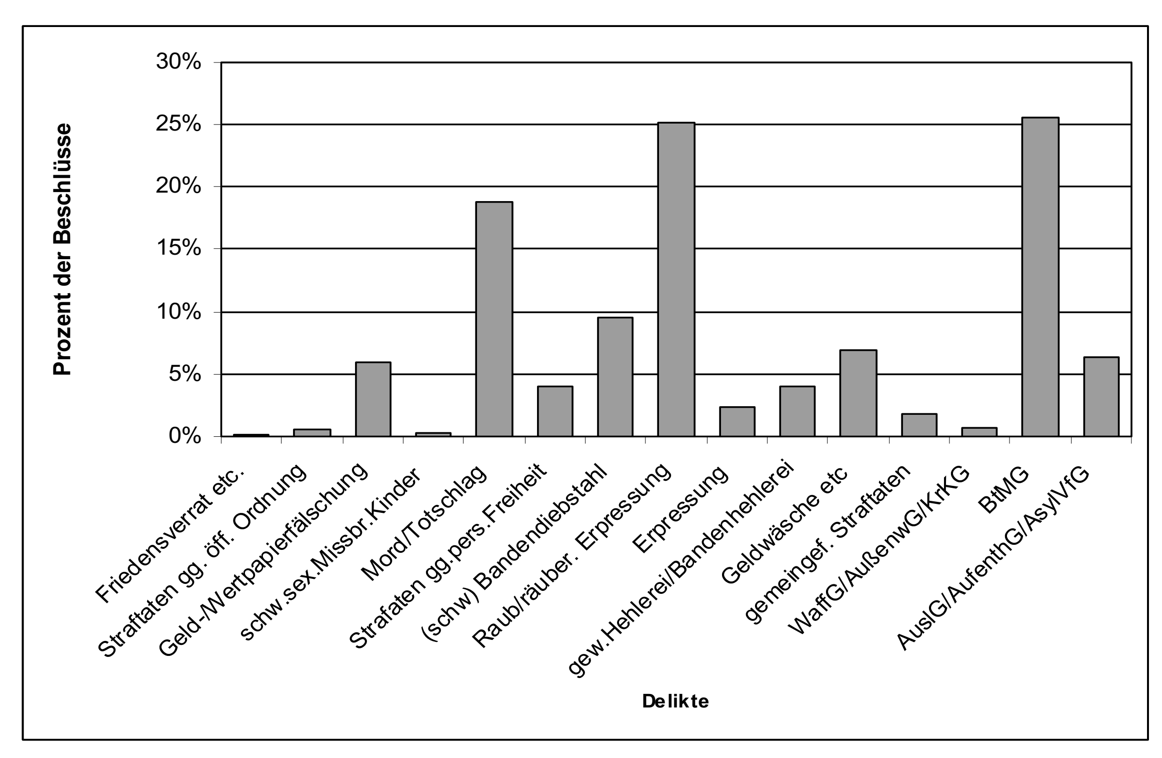
Aus Abbildung 30 ergeben sich die Katalogdelikte im Einzelnen. Am häufigsten lagen den Beschlüssen von den Katalogdelikten Rauschgiftdelikte (25,6 Prozent der Fälle, N = 232) sowie Raub und räuberische Erpressung (25,1 Prozent der Fälle, N = 228) zugrunde. Sehr oft gaben zudem Mord- und Totschlagsdelikte (18,8 Prozent der Fälle, N = 171) Anlass für die Anordnung der Verkehrsdatenabfrage. (Schwerer) Bandendiebstahl lag in 9,6 Prozent der Fälle (N = 87) und Geldwäsche in 6,9 Prozent der Fälle (N = 63) zugrunde. In 6,4 Prozent der Fälle (N = 58) waren Verstöße gegen das Aufenthaltsgesetz (früher AuslG) und in 5,9 Prozent der Fälle (N = 54) Geld- und Wertpapierfälschungen Grund für die Anordnungen. In je 4 Prozent der Fälle (N = 36) waren die Beschlüsse durch Straftaten der Banden- und gewerbsmäßigen Hehlerei sowie Straftaten gegen die persönliche Freiheit begründet. Selten kamen an Katalogdelikten Erpressung (2,4 Prozent der Fälle), gemeingefährliche Straftaten (1,8 Prozent der Fälle), Verstöße gegen das Waffengesetz oder Außenwirtschaftsgesetz (0,7 Prozent der Fälle), Straftaten gegen die öffentliche Ordnung (0,6 Prozent der Fälle), schwerer sexueller Missbrauch von Kindern (0,3 Prozent der Fälle) sowie Friedensverrat o. ä. (0,1 Prozent der Fälle) vor. Von den Katalogdelikten wurden 82 Prozent der Erpressungen (insg. 22 Fälle) mittels Endeinrichtung begangen. Die räuberischen Erpressungen wurden teilweise mittels Endeinrichtung verübt (neun Fälle – 4 Prozent der Kategorie Raub/räuber. Erpressung).

Wie schon erwähnt lagen 28 Prozent der Anordnungen keine Katalogdelikte, sondern andere Straftaten zugrunde

Abbildung 30



Verteilung der Katalogtaten auf die Beschlüsse



und weiteren 2 Prozent zumindest auch eine andere Straftat. Um welche Delikte es sich dabei im Einzelnen handelte, kann Abbildung 31 entnommen werden.

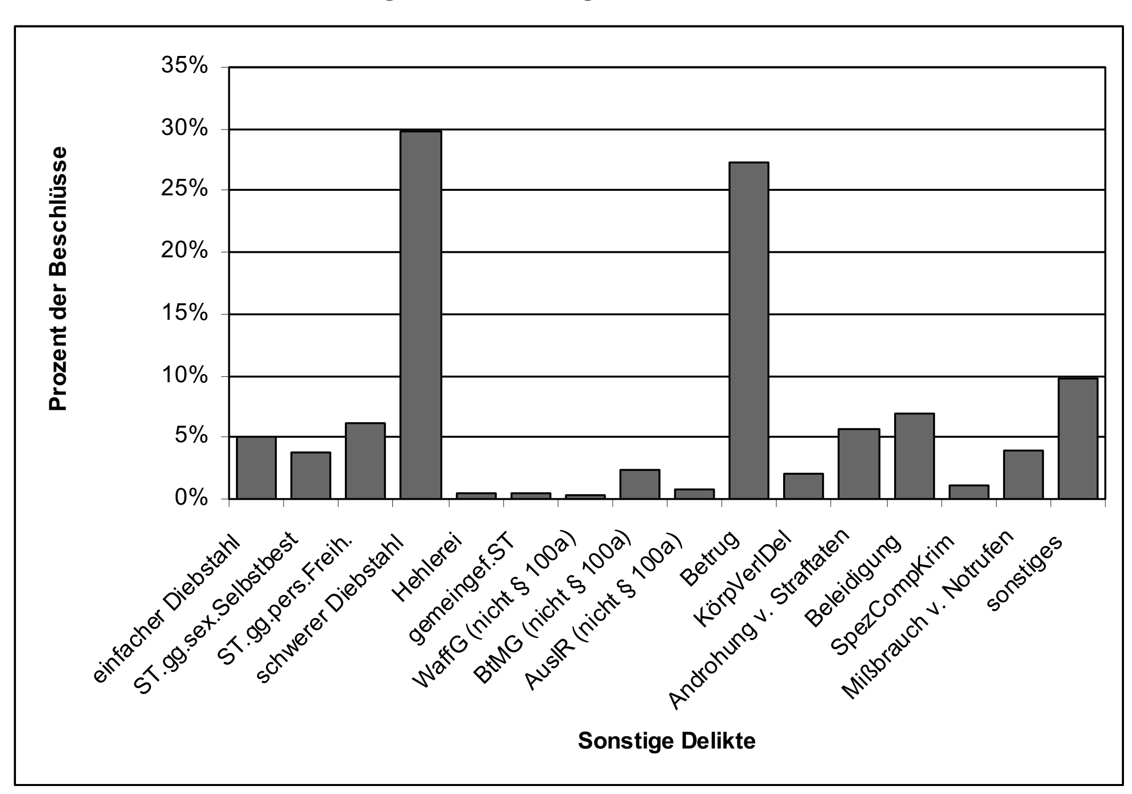
Dabei waren schwere Diebstahlsdelikte, die nicht unter den Katalog des § 100a Satz 1 StPO fallen (überwiegend § 243 StGB, 29,8 Prozent der Fälle, N = 111) und Betrug (27,3 Prozent der Fälle, N = 102) die am häufigsten zugrunde liegenden Nichtkatalogtaten. Zu 7,0 Prozent gaben Beleidigungen (N = 26) und zu 6,2 Prozent Straftaten gegen die persönliche Freiheit (§§ 239, 240, 241 StGB, N = 23) Anlass für die Anordnung der Maßnahmen. Weniger häufig kamen Androhung von Straftaten (5,6 Prozent der Fälle, N = 21), einfacher Diebstahl (5,1 Prozent der Fälle, N = 19), Missbrauch von Notrufen (4,0 Prozent der Fälle, N = 15) und Straftaten gegen die sexuelle Selbstbestimmung (3,8 Prozent der Fälle, N = 14) vor. Am seltensten waren Rauschgiftdelikte, die nicht unter den § 100a-Katalog fallen (2,4 Prozent der Fälle), Körperverletzungsdelikte (2,1 Prozent der Fälle) sowie Computerkriminalität (§ 202 StGB usw. – 1,1 Prozent der Fälle). In etwa 12 Prozent der Fälle wurden sonstige Straftaten wie Hehlerei, gemeingefährliche Straftaten, Vorteilsannahme, Bestechlichkeit, Urkundenfälschung, Amtsanmaßung, Vortäuschen einer Straftat sowie Straftaten nach §§ 373, 374 AO als Grundlage für die Anordnungen herangezogen.

Bei den Nicht-Katalogtaten wurden Hehlerei, gemeingefährliche Straftaten, einfacher Diebstahl, schwerere Diebstähle sowie Rauschgiftdelikte nie mittels Endeinrichtung begangen. Dagegen wurden Telefon, Computer, etc. beim Missbrauch von Notrufen, bei Computerkriminalität, bei der Androhung von Straftaten und der Beleidigung immer (100 Prozent) verwendet. Ebenfalls häufig wurden Endeinrichtungen bei Straftaten gegen die persönliche Freiheit (Bedrohung, Nötigung per Telefon – 91 Prozent), bei Betrugsdelikten (53 Prozent) sowie bei Straftaten gegen die sexuelle Selbstbestimmung (sexuelle Belästigung vor allem von Kindern am Telefon, 36 Prozent) eingesetzt. Bei den Körperverletzungsdelikten kam die Begehung mittels Telefon nur in einem Fall vor (Telefonterror, 12,5 Prozent). Bei den sonstigen Fällen wurden die Amtsanmaßungen per Telefon begangen.

Hehlerei, gemeingefährliche Straftaten, schwerere Diebstahlsdelikte sowie Rauschgiftdelikte lassen sich unter den Begriff der Straftat von erheblicher Bedeutung subsumieren. Einfache Diebstähle dagegen werden im Regelfall – abhängig vom Wert des Diebstahlsobjekts – nicht von dem Begriff erfasst. Bei den Straftaten gegen die persönliche Freiheit wurden die geringfügigeren Delikte wie Nötigung oder Bedrohung immer mittels Endeinrichtung begangen. Die anderen Delikte (§ 239 StGB) waren als erheblich anzusehen.

Abbildung 31





3. Experteninterviews

Auch bei den Experteninterviews wurden die Befragten nach typischen Kriminalitätsformen oder Fallkonstellationen gefragt, bei denen die Verkehrsdatenabfrage eine besonders hohe Bedeutung hat. Es sollten die Delikte genannt werden, in denen diese Ermittlungsmaßnahme besonders häufig zur Anwendung kommt.

a) Polizeibeamte

(1) Typische Kriminalitätsformen

Als typische Kriminalitätsformen, bei denen eine Auskunftserteilung über Verkehrsdaten eine besonders große Rolle spielt, wurden von den befragten Polizeibeamten an erster Stelle Raub, Rauschgiftkriminalität und Formen der organisierten Kriminalität angegeben. Bei den Raubdelikten wurden „Raub“, „Raub von Mobiltelefonen“ und „Bankraub“ genannt. Gerade Funkzellenabfragen seien bei Banküberfällen o. ä. von erheblicher Bedeutung, da die Täter sich vor Ort absprechen würden. Einen Schwerpunkt bildeten auch der Raub von Mobiltelefonen und die dabei angewandten IMEI-Abfragen. Bei Betäubungsmitteldelikten könne man anhand der Daten Handels- und Geschäftsstrukturen erkennen und Standorte feststellen, was vor allem bei Einfuhrschmuggel bedeutend sei. Alle Taten, bei denen der Täter mobil ist und wo illegale Waren transportiert werden, wurden ebenfalls als typische Fallkonstellationen genannt. Weiter wurde ganz allgemein auf Kapitalverbrechen verwiesen, insbesondere Tötungsdelikte. In der Regel seien dies Beziehungsdelikte bzw. es habe in der Regel vor der Tat Kontakt zwischen Täter und Opfer gegeben. Typische Kriminalitätsformen seien zudem Bandendelikte, gewerbsmäßige (Banden-) Hehlerei, Wohnungseinbrüche sowie Bandendiebstähle. Bei Wohnungseinbrüchen würden die Verkehrsdaten im Hinblick das sog. „home checking“ bedeutsam, bei dem der Täter vor dem Einbruch beim Opfer anruft, um zu prüfen, ob jemand in der Wohnung ist. Weiter wurden Erpressung, Entführung, Vermisstensachen und Sexualdelikte aufgeführt. Allgemeiner wurde formuliert, dass die Maßnahmen bei allen Formen der Schwerstkriminalität bedeutsam seien. Alle Straftaten, bei denen mehrere Täter agieren, seien für §§ 100g, 100h-Maßnahmen typisch. Ebenso sei dies immer dann der Fall, wenn der Täter telefonisch Straftaten mit anderen verabrede. Eine besonders große Bedeutung würde die Verkehrsdatenabfrage auch dann einnehmen, wenn zwingend zwischen Tatbeteiligten Kommunikation stattfindet. Das sei in der Regel der Fall, wenn mehrere Täter arbeitsteilig (wie bei Betäubungsmitteldelikten) über Distanzen kommunizieren müssen. Es sei zu erwarten, dass beweisrelevante Kommunikation geführt wird und daher seien die Aufzeichnung der Gespräche und die Verkehrsdaten bedeutend. Im Bereich der Internetkriminalität würden die Ermittlungen nicht voranschreiten ohne Verkehrsdatenabfrage. Dort hätten die Maßnahmen eine sehr hohe Bedeutung. Es sei die einzige Möglichkeit, um einen Täter zu ermitteln. Gerade in Betrugsfällen spiele das Internet eine große Rolle. Ebenso sei die Maßnahme im Bereich der Kinderpornographie bedeutsam. Das Internet sei das herausragende Mittel für den Austausch. In diesen Fällen sei zur Ermittlung des Täters nur eine Verkehrsdatenabfrage erfolgversprechend. Allgemein sei §§ 100g, 100h StPO bei allen Straftaten mittels Endeinrichtung bedeutsam.

(2) Straftat von erheblicher Bedeutung

Fast alle der befragten Polizeibeamten möchten den Begriff der Straftat von erheblicher Bedeutung mit dem Verweis auf den Katalog des § 100a StPO beibehalten. Der Begriff habe sich etabliert und in der Praxis bewährt. Der Begriff der Straftat von erheblicher Bedeutung sei zwar ein „Kaugummibegriff“, ein unbestimmter Rechtsbegriff, der von Fall zu Fall ausgelegt werden müsse. Es sei unklar, was unter diesen schwammigen Begriff falle. Trotzdem seien damit keine schlechten Erfahrungen gemacht worden. Der Begriff sei durch Urteile eingegrenzt worden. Die Einzelfallprüfung sei wichtig. Ein Katalog sei wohl einfacher handhabbar, eindeutiger und nachvollziehbarer. Er wäre zur Rechtssicherheit der handelnden Behörden von Vorteil. Aber der Begriff der Straftat von erheblicher Bedeutung biete mehr Spielraum zur Auslegung. Ein Katalog berge immer die Gefahr, dass Straftaten nicht erfasst werden, die im Einzelfall erheblich sind und bei denen die Maßnahme notwendig wäre. Dann würde versucht, die Delikte unter den Katalog zu subsumieren und sie würden als schwerer dargestellt, als sie eigentlich seien. Ein Katalog müsste ständig verändert werden. Es komme immer wieder zu neuen Formen der Durchführung von Straftaten, gerade im Bereich der Computerkriminalität. Ein fester Katalog berge deshalb die Gefahr, dass Entwicklungen und Veränderungen in den Erscheinungsformen der Kriminalität nicht berücksichtigt werden könnten. Der Ermessenspielraum der Justiz sollte hier beibehalten werden. Auslegungsmöglichkeit und Interpretationsspielraum hätten erhebliche Bedeutung.

Zwei der Befragten halten einen festen, klaren Katalog für besser. Dies ließe weniger Raum für Interpretationen und sei einer Situation vorzuziehen, in der darüber gestritten werden müsse, ob es sich um eine Straftat von erheblicher Bedeutung handle oder nicht. Das würde auf alle Fälle zu mehr Rechtssicherheit führen. Auf Änderungen könne man nachträglich durch Anpassungen reagieren.

b) Staatsanwälte

(1) Typische Kriminalitätsformen

Die befragten Staatsanwälte gaben als typische Kriminalitätsformen, bei denen die Verkehrsdatenabfrage eine besondere Bedeutung hat, Rauschgiftkriminalität, Organisierte Kriminalität, Bandendelikte, bandenmäßig begangene Raubüberfälle, Handyraubfälle, Diebstähle in besonders schwerem Fall (insb. Wohnungseinbruchsdiebstahl), Tötungsdelikte, betrügerische Anmietung von Kfz sowie alle Straftaten, die mittels Telekommunikationseinrichtung begangen werden (z. B. Drohanrufe, Erpressung, Bombendrohung, Beleidigung) an. Ein Befragter schilderte die Bedeutung der Daten für Brandstiftungsfälle an

Hand eines Falles, in dem der verdächtige Hauseigentümer Kontakt zu den engagierten Brandstiftern aufnehme und mit der Verkehrsdatenabfrage die Täter dann überführt werden könnten. Ebenso sei die Abfrage bei solchen Straftaten bedeutsam, die ausschließlich über Internet begangen werden können (Datenveränderung, Computersabotage, Phishing, Betrugsstraftaten im Internet). Die Abfrage der Daten spiele bei allen Straftaten, die konspirativ durchgeführt und bei denen mehreren Personen tätig würden, eine wichtige Rolle.

(2) Straftat von erheblicher Bedeutung

Ein fester Katalog von Straftaten wird von den meisten befragten Staatsanwälten abgelehnt. Der Begriff der Straftat sei zwar etwas schwammig und auslegungsbedürftig, aber trotzdem zu befürworten. Ein abschließender Katalog sei nicht praktikabel. Ebenso wie bei dem Katalog des § 100a StPO, müsste man ihn immer wieder ergänzen. Man würde versuchen, die Vorschriften zu umgehen, z. B. bandenmäßige Begehung feststellen. Flexibilität sei erforderlich. Natürlich sei problematisch, was erheblich ist und eine Kontrolle durch die Gerichte sei erforderlich, denn es dürfe nicht zur Ausuferung kommen. Der unbestimmte Rechtsbegriff müsse entsprechend begründet werden. Was davon erfasst ist, sei vom Beurteiler abhängig, aber es seien mehrere Personen an der Prüfung beteiligt. Zudem sei so gewährleistet, dass die Maßnahmen nicht bei jedem Ladendiebstahl durchgeführt werden. Durch die Bezugnahme auf den Katalog des § 100a StPO ließe sich eine Wertung entnehmen, was unter dem Begriff zu verstehen sei. Dadurch würde der Anwendungsbereich etwas eingegrenzt.

Zwei Befragte würden einen festen Katalog befürworten. Damit würden Unklarheiten beseitigt. Allerdings müsse dieser Katalog erheblich ausgeweitet werden. Da der § 100g StPO im Verhältnis zu § 100a StPO weniger eingriffsintensiv ist, sollte dessen Katalog viel umfassender sein. Zwei Befragte meinen, dass ein fester Katalog zwar zur Rechtssicherheit und Rechtsklarheit beitragen würde. Nachteil sei aber, dass der Katalog ständig nachgebessert werden müsste. Es wären immer wieder Erweiterungen notwendig. Die Gesetzgebung schreite voran und eine Nachbesserung sei immer nur mit Zeitverzug möglich.

c) Richter

(1) Typische Kriminalitätsformen

Nach Angabe der befragten Richter findet die Auskunftserteilung über Verkehrsdaten vor allem bei Betäubungsmitteldelikten, Tötungsdelikten, organisierter Kriminalität, Betrugsfällen im Internet oder per Telefon (z. B. Enkeltrick), Handyraubfällen, bei Raub und räuberischem Diebstahl, Internetkriminalität, bei Entführungsfällen, Erpressung, Bedrohung, Kinderpornographie, Stalking, Autoschieberringen sowie Bandendelikten Anwendung. Es würden Absprachen stattfinden, so dass man feststellen könne, ob der Täter am Tatort war. In Berlin würde der Raub von Mobiltelefonen den größten Teil an 100gh-Fällen einnehmen. Immer wenn es um kriminelle Vereinigungen und um die Aufdeckung von Strukturen gehe, habe die Auskunftserteilung eine besonders große Bedeutung. Bei Betäubungsmittelsachen würde die Abfrage der Daten häufig zusammen mit einer Telekommunikationsüberwachung angeordnet. Man könne die Netze, die Kontakte zwischen den Tätern aufdecken. Ein Befragter gab auch den Diebstahl von Mobiltelefonen als häufige Fallgruppe an. Eher unbedeutend sei die Maßnahme dagegen bei Beleidigungen, da diese Anträge zumeist sowieso wegen Geringfügigkeit abgelehnt würden, gab ein weiterer Befragter an. Im Übrigen sei der Beschuldigte in diesen Fällen oft bekannt und seine Vernehmung sinnvoller.

(2) Straftat von erheblicher Bedeutung

Die meisten der befragten Richter befürworten keinen festen Katalog. Der Begriff der Straftat von erheblicher Bedeutung sei zwar „schwammig“. Man müsse überlegen, ob z. B. eine Beleidigung wirklich eine Straftat von erheblicher Bedeutung ist. Es gebe unterschiedliche Interpretationsmöglichkeiten, z. B. anhand des Strafmaßes oder des Rechtsguts. Der Begriff sei „schillernd“. Es handle sich um ein „Einfallstor“ und man könne alles darunter subsumieren. Trotzdem sei ein fester Katalog von Straftaten nicht zu befürworten. Die Ermittlungsmaßnahme müsse vom Einzelfall abhängig gemacht werden. Ein fester Katalog verbaue die Möglichkeit, zur Aufklärung von Massendelikten (z. B. Raub von Mobiltelefonen). Dann würde die generalpräventive Warnfunktion der Strafverfolgung entfallen. Ein Katalog sei immer eindeutiger, berge aber die Gefahr, dass Fälle nicht erfasst würden, bei denen die Verkehrsdatenabfrage sinnvoll und gerechtfertigt gewesen wäre. Manche Delikte würden durch das Raster fallen. Eine Verhältnismäßigkeitsprüfung reiche. Es sei nicht möglich, alles gesetzlich zu regeln. Eine offene Klausel, die man ausfüllen müsse, sei für die Praxis besser.

Zwei Befragte finden den Begriff der Straftat von erheblicher Bedeutung als zu „schwammig“. Ein fester Straftatenkatalog sei zu befürworten. Ein Verweis auf die Straftaten in § 100a StPO sei sinnvoll. Begründet wird dies damit, dass es immer wieder Streitigkeiten mit der Polizei und der Staatsanwaltschaft gebe, ob die Straftat nun erheblich ist oder nicht. Es sei nicht zu verstehen, warum in § 100a StPO der Katalog an Straftaten festgelegt sei, in § 100g aber nur der Begriff der Straftat von erheblicher Bedeutung. Es sei nicht Aufgabe der Richter, sondern des Gesetzgebers, den unbestimmten Begriff näher zu umgrenzen. Es könne nicht sein, dass der eine bestimmte Straftaten darunter subsumiert und der andere nicht. Ein Katalog könne je nach Praxiserfahrung erweitert werden und wäre für die Rechtssicherheit besser, auch wenn damit ein gewisser Aufwand verbunden wäre.

Ein Richter gab an, dass er nicht begreife, warum z. B. bei einem Diebstahl von Mobiltelefonen §§ 100g, 100h StPO nicht angewendet werden können. Es sei die einfachste Möglichkeit der Aufklärung. Ein anderer Befragter schlägt die Formulierung vor: „wo es zur Sachverhaltsaufklärung erheblich beiträgt und es verhältnismäßig ist“.

d) Verteidiger

(1) Typische Kriminalitätsformen

Die befragten Verteidiger wurden nach Verfahren befragt, in denen sie mit den Maßnahmen nach §§ 100g, 100h StPO konfrontiert wurden. Dabei wurden ganz überwiegend Betäubungsmittel- und organisierte Kriminalität-Verfahren, Verfahren wegen Verbreitung (kinder-)pornographischer Schriften, wegen Einschleusungskriminalität, wegen Mordes und wegen Betruges genannt.

(2) Straftat von erheblicher Bedeutung

Alle befragten Verteidiger halten erwartungsgemäß einen festen Straftatenkatalog für vorzugswürdig. Der Begriff der Straftat von erheblicher Bedeutung sei äußerst schwammig. Er sei zu vage und niemand wisse, was darunter falle. Alternativ sei nach Ansicht eines Befragten noch eine klare Regelung mit Definitionen im allgemeinen Teil denkbar. Ein Kriterienkatalog wird von einem Befragten ausdrücklich nicht befürwortet. Wünschenswert sei auch eine Präzisierung bzgl. der mittels Endeinrichtung begangenen Straftaten, um Bagatelldelikte auszuschließen.

e) Telekommunikationsunternehmen

(1) Typische Kriminalitätsformen

Zwei Mitarbeiter der befragten Telekommunikationsunternehmen gaben zu den zugrunde liegenden Delikten an, dass diejenigen Deliktsformen, die in der Öffentlichkeit in der Regel als Begründung für die Notwendigkeit dieses Ermittlungsinstruments herangezogen werden würden, insbesondere der Terrorismus und die Bekämpfung von Kinderpornographie, eher selten seien. Stattdessen werde die Abfrage ganz überwiegend wegen Betäubungsmitteln im Bagatellbereich angeordnet. Was zu Beginn ein Verstoß gegen das Arzneimittelgesetz gewesen sei, werde später als gewerbsmäßige Bandenhehlerei dargestellt. Die Begründung, es gehe um Schwerstkriminalität, gehe nach ihrer persönlichen Erfahrung an der Realität vorbei. Im Festnetzbereich, führt einer der Befragten aus, gehe es vor allem um Betäubungsmittel und im Internetbereich um Betrug und Urheberrechtsverletzungen.

(2) Straftat von erheblicher Bedeutung

Fast alle befragten Mitarbeiter der Telekommunikationsanbieter meinen, es sei unklar, was eine Straftat von erheblicher Bedeutung sei. Der Begriff sei kein wirkliches Regulativ. Es gebe kaum eine Straftat, wo die Maßnahme nicht angewandt werde. Die Grenzziehung sei schwierig. Die Eingriffsschwelle sollte höher gesetzt werden, da es sich um einen sehr weitgehenden Eingriff handle. Es gebe keinen großen Unterschied zu der Überwachung der Inhalte. Die Möglichkeit der Anordnung bei mittels Endeinrichtung begangenen Straftaten sollte entfallen. Die Abfrage der Daten sollte nur bei schweren Straftaten möglich sein. Mittels Endeinrichtung begangene Taten könnten über § 101 TKG abgehandelt werden. Eine Fangschaltung reiche z. B. bei Stalking aus. Eine Lücke würde nur bei einem einmaligen Vorfall entstehen. Es sei absurd, dass eine bloße Beleidigung ausreiche, um in das Grundrecht auf Wahrung des Fernmeldegeheimnisses einzugreifen, meint einer der Befragten. Ein weiterer Befragter führt aus, dass der Diebstahl eines Mobiltelefons keine erhebliche Straftat sei.

4. Zusammenfassung der Ergebnisse

Im Rahmen der schriftlichen Befragung wurde von den Staatsanwälten angegeben, dass die am häufigsten den Anträgen zugrunde liegenden Straftaten von erheblicher Bedeutung Betäubungsmitteldelikte, Raub und räuberische Erpressung, Diebstahlsdelikte und Betrugsdelikte sind. Bei den mittels Endeinrichtung begangenen Straftaten wurden Computerbetrug sowie Beleidigung und Bedrohung als die relevantesten Anlassdelikte benannt, für die Beschlüsse nach §§ 100g, 100h StPO beantragt wurden. Die Verbreitung pornographischer Schriften, die häufig im Zusammenhang mit der Verkehrsdatenabfrage erwähnt wird, spielt hingegen eine nur untergeordnete Rolle. Diese Einschätzung deckt sich mit den Ergebnissen der Aktenanalyse. Die häufigsten den Anordnungen tatsächlich zugrunde liegenden Katalogdelikte waren Betäubungsmittel-Strafsachen, Raub und räuberische Erpressung, sowie Mord und Totschlag. Sonstige Anlassdelikte stellen vor allem besonders schwere Fälle des Diebstahls und Betrugsdelikte dar. Letztere wurden nicht mittels Endeinrichtung begangen. Typische Computerkriminalität war dagegen selten und die Verbreitung pornographischer Schriften nie Grund für die Anordnung der Maßnahmen nach §§ 100g, 100h StPO. Zu berücksichtigen ist dabei, dass ein Anstieg der Abfrage Bestandsdaten zu dynamischen IP-Adressen vor allem im Jahr 2005 zu bemerken war, die untersuchten Akten aber aus den Jahren 2003 und 2004 stammten. Trotzdem war auch schon in diesen Jahren die Nutzung von Computer und Internet sehr verbreitet. Bedrohungen und Beleidigungen gaben entgegen den Einschätzungen aus der schriftlichen Befragung nur selten Anlass zur Anordnung der Maßnahmen nach §§ 100g, 100h StPO. Von den befragten Experten gaben Polizeibeamte, Staatsanwälte, Richter und Verteidiger übereinstimmend an, dass den Anordnungen nach §§ 100g, 100h StPO vor allem Betäubungsmittelstraftaten, Raubdelikte, organisierte Kriminalität, Tötungsdelikte, Betrugsstrafsachen im Internet sowie Verbreitung kinderpornographischer Schriften zugrunde liegen. Die Telekommunikationsunternehmen dagegen meinten, dass letztere kaum in den Beschlüssen vorkämen. Dies wird durch die Ergebnisse der Aktenauswertung bestätigt.

Die Meinungen der mittels Fragebogen befragten Staatsanwälte gehen hinsichtlich des Begriffs der Straftat von erheblicher Bedeutung und des Verweises auf den Straftatenkatalog des § 100a Satz 1 StPO auseinander. Zwar überwiegt der Anteil derjenigen, die den Gesetzestext in dieser Hinsicht in seiner aktuellen Fassung beibehalten wollen (60 Prozent der Befragten). Von den übrigen 40 Prozent werden jedoch verschiedene Verbesserungsvorschläge unterbreitet. Der Großteil dieser 40 Prozent möchte den Gesetzeswortlaut auf den Begriff der Straftat von erheblicher Bedeutung beschränken. Verbunden ist

damit wohl auch eine Angleichung an die sich aus den Akten abbildende Praxis sowie die Auffassung, dass es sich bei der Verkehrsdatenabfrage um ein an Bedeutung gerade für allgemeine Kriminalität zunehmendes Instrument der Ermittlungen handelt. In Bezug auf die zweite Variante des § 100g I StPO, der mittels Endeinrichtung begangenen Straftat, gehen drei Viertel der schriftlich befragten Staatsanwälte mit der h. M. in der Literatur davon aus, dass eine mittels Endeinrichtung begangene Straftat nicht von erheblicher Bedeutung sein muss.

Die interviewten Polizeibeamten, Staatsanwälte und Richter befürworten überwiegend den Begriff der Straftat von erheblicher Bedeutung und den Verweis auf den Katalog des § 100a Satz 1 StPO. Der Begriff sei zwar auslegungsbedürftig, aber praxisgerechter als ein fester Katalog. Eine abschließende Festlegung von Straftaten könnte den ständigen technischen Fortentwicklungen nicht gerecht werden und müsste immer wieder verändert werden. Im Einzelfall erhebliche Straftaten könnten dann nicht aufgeklärt werden. Verteidiger und Telekommunikationsanbieter dagegen befürworten einen festen Straftatenkatalog. Es sei unklar, was unter den Begriff der Straftat von erheblicher Bedeutung falle. Zudem halten diese Interviewten sowie die befragten Datenschützer einen Ausschluss von Bagatelldelikten für notwendig.

II. Initiative und Ablauf von Anregung bis Anordnung der Maßnahme

In diesem Abschnitt werden die Ergebnisse zum Ablauf der Beantragung der Verkehrsdatenabfrage erörtert. Dabei sollen die Interaktionen zwischen Polizei, Justiz und Netzbetreibern bis zur Anordnung der Maßnahme dargestellt werden.

1. Schriftliche Befragung

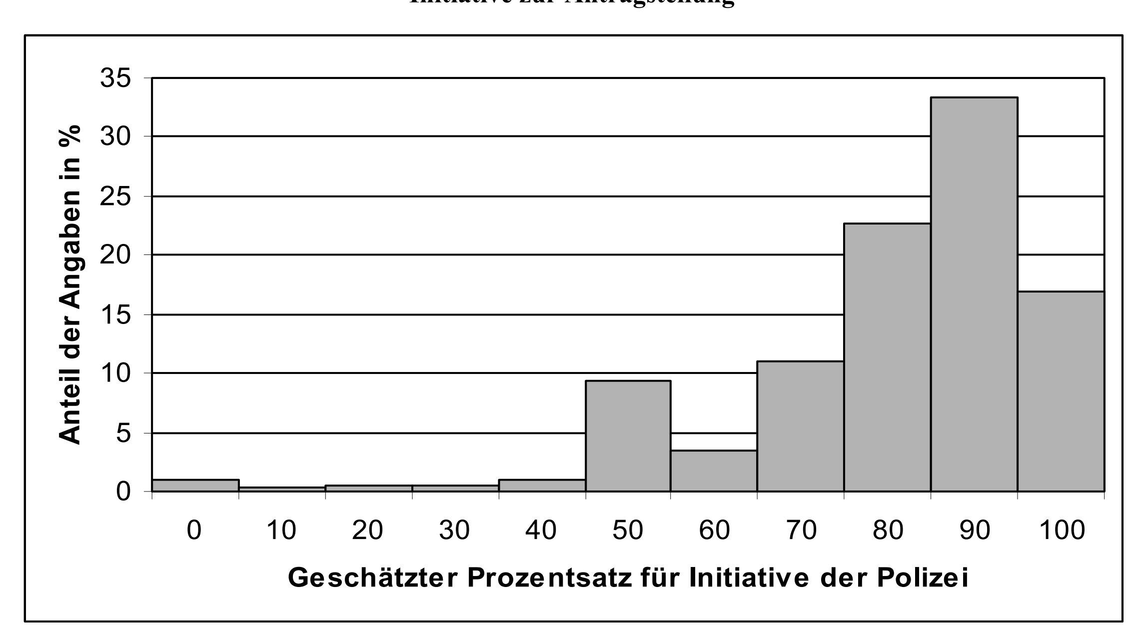
a) Initiative zur Antragstellung

Wie sich aus Abbildung 32 ergibt, sieht die große Mehrheit der Befragten die Polizei als maßgeblichen Initiator der Maßnahme an. 17 Prozent der Befragten (N = 131) nahmen an, dass die Initiative zu 100 Prozent von der Polizei ausgehe. 33 Prozent der Befragten (N = 257) gehen davon aus, dass die Polizei die Maßnahme zu 90 Prozent veranlasst und 23 Prozent der Befragten (N = 174) schätzen, dass die Polizei in 80 Prozent der Fälle Initiator ist.

Nur 3,4 Prozent der Befragten meinten hingegen, dass in über 50 Prozent der Fälle die Staatsanwaltschaft die Antragstellung selbst initiiere. 10 Prozent sahen die Initiative zur Antragstellung zu gleichen Teilen auf Polizei und Staatsanwaltschaft verteilt.

Abbildung 32

Initiative zur Antragstellung



b) Antragstellung

In Tabelle 19 sind die staatsanwaltschaftlichen Abteilungen, in denen nach Einschätzung der Befragten Maßnahmen nach §§ 100g, 100h StPO beantragt bzw. im Falle einer Eilanordnung angeordnet werden, spezifiziert. Hierbei wurden die Anzahl der Nennungen in den verschiedenen Kategorien sowie die Gesamtsumme angegeben, des Weiteren der Mittelwert über die Nennungen.

Besonders häufig wurden die drei vorgegebenen Dezernate organisierte Kriminalität, Betäubungsmittelkriminalität sowie Wirtschaftskriminalität genannt. Dabei werden in organisierte Kriminalität- und Betäubungsmittel-Dezernaten nach Angaben der Befragten häufig Verkehrsdatenabfragen beantragt, während dies in Wirtschaftsabteilungen eher seltene bis gelegentliche Vorgänge sind. Die weiteren aufgeführten Dezernate wurden von den Befragten selbst unter sonstige aufgeführt. Am häufigsten wurde hier noch das allgemeine Dezernat genannt mit gelegentlichen Anträgen. Auch in der Abteilung für Kapitaldelikte werden die Maßnahmen gelegentlich bis häufig beantragt. Etwa 20 Nennungen hatten die Dezernate Sexualdelikte, Raub bzw. räuberische Erpressung, Jugendkriminalität, Computerdelikte, Betrugssachen sowie (Kinder-) Pornographie, wobei die Abteilung für Computerdelikte auffällt, da dort eine wohl deliktsspezifisch hohe Antragsdichte angenommen wird[434].

[434] Der Mittelwert bei den Brandstiftungsdelikten entfaltet wegen der geringen Anzahl der Nennungen keine Aussagekraft.

Tabelle 19

Abteilungen der StA, in denen Verkehrsdatenabfragen beantragt werden

	nie (1)	selten	gelegentlich	häufig	immer (5)	Summe	Mittel
Organisierte Kriminalität	1		30	539	65	635	*4,1*
Betäubungsmitteldelikte		2	83	538	19	642	*3,9*
Wirtschaftsdelikte	20	204	192	61	1	478	*2,6*
Allgemeine Kriminalität	2	44	82	34		162	*2,9*
Kapitaldelikte		4	11	27	3	45	*3,6*
Sexualdelikte			18	6		24	*3,3*
Raub/(räuber.) Erpressung			12	11	1	24	*3,5*
Jugendkriminalität		6	14	2		22	*2,8*
Computerkriminalität			1	16	4	21	*4,1*
Betrug		1	7	8	2	18	*3,6*
(Kinder)Pornographie			6	9	2	17	*3,8*
Schleusung			4	5		9	*3,6*
Verkehrsdelikte	4	3				7	*1,4*
Brandstiftung				2	1	3	*4,3*
Sonstige		13	25	20	4	62	*3,2*

2. Aktenanalyse

a) Initiative zur Antragstellung

Die Auswertung der Akten ergab, dass die Initiative zur Beantragung einer Maßnahme nach §§ 100g, 100h StPO tatsächlich zu 91 Prozent von der Polizei und zu 9 Prozent von der Staatsanwaltschaft ausging (Abbildung 33). Dabei ist jedoch zu berücksichtigen, dass – wie unten näher dargestellt wird – vor der Antragstellung häufig Besprechungen zwischen Polizei und Staatsanwaltschaft stattgefunden haben. In diesen Fällen kann es durchaus sein, dass die Initiative auf den Überlegungen aller Beteiligten beruht.

Die Akten ließen keine Aussage über die Abteilungen innerhalb der Polizei und der Staatsanwaltschaft, in denen die Maßnahmen angeordnet wurden, zu. In den wenigsten Fällen wurde explizit aufgeführt, um welche Abteilung es sich handelte. Oftmals enthielten die Akten nur Dezernatsnummern.

b) Besprechungen

Besprechungen vor Antragstellung oder Beschlusserlass fanden bei 106 Beschlüssen statt (8 Prozent der Beschlüsse). Es ist zu berücksichtigen, dass dies zumindest die Fälle sind, die ausdrücklich in den Akten vermerkt sind. Dabei handelte es sich in 83 Prozent der Fälle um Besprechungen zwischen Polizei und Staatsanwaltschaft, in 11 Prozent der Fälle um Besprechungen zwischen Staatsanwaltschaft und Richter und in 6 Prozent der Fälle um Besprechungen zwischen Polizei und Gericht. Bei den Absprachen zwischen Polizei und Staatsanwaltschaft handelte es sich meist um die Unterredung über das weitere Vorgehen, in deren Verlauf erörtert wurde, ob ein Antrag nach §§ 100g, 100h StPO gestellt werden soll oder nicht. Besprechungen zwischen Staatsanwaltschaft und Gericht betrafen Fälle, in denen der Richter die Staatsanwaltschaft darauf hinwies, dass ein Beschluss nach §§ 100g, 100h StPO notwendig sei oder der Antrag so nicht korrekt sei. Weiterer Inhalt der Gespräche war, dass der Beschluss noch auf weitere Anschlüsse ausgedehnt werden muss. Zwischen Polizei und Gericht ging es um Änderungen hinsichtlich des Abfragezeitraums, weil z. B. ein weiterer Drohanruf eingegangen war.

c) Zeitlicher Ablauf von der Antragstellung bis zur Anordnung

Aus der Aktenanalyse ergibt sich, dass meist die Polizei die Maßnahme anregt, dann die Staatsanwaltschaft einen Antrag auf Durchführung einer Verkehrsdatenabfrage stellt und daraufhin ein Beschluss durch den Richter erlassen wird. Wie viel Zeit zwischen Anregung einer Verkehrsdatenabfrage durch die Polizei und Beantragung der Maßnahme durch die Staatsanwaltschaft vergeht, ist in Abbildung 34 dargestellt. In 48 Prozent der Fälle erfolgen Anregung und Antragstellung innerhalb eines Tages. Ein Tag vergeht in 15 Prozent der Fälle zwischen Anregung und Beantragung der Maßnahme. Bei 81 Prozent der Beschlüsse erfolgt die Beantragung daher innerhalb von sechs Tagen nach der Anregung, bei 10 Prozent zwischen sieben und 14 Tagen und bei 9 Prozent dauerte es länger als 14 Tage.

Sehr ähnlich gestaltet sich das Bild bei der Zeit, die zwischen Beantragung der Maßnahme und Erlass des Beschlusses durch den Richter vergeht (Abbildung 35). Auch hier ergeht der Beschluss größtenteils noch am Tag der Antragstellung (51 Prozent). Hier ergeht der Beschluss sogar bei 88 Prozent innerhalb von sechs Tagen nach Beantragung.

Dementsprechend vergeht auch zwischen Anregung und Beschlusserlass in 52 Prozent der Fälle nicht mehr als ein Tag. Hier erfolgte bei 74 Prozent der Beschlüsse die Anordnung innerhalb von sechs Tagen nach Anregung der Maßnahmen.

Abbildung 33



Initiative zur Antragstellung

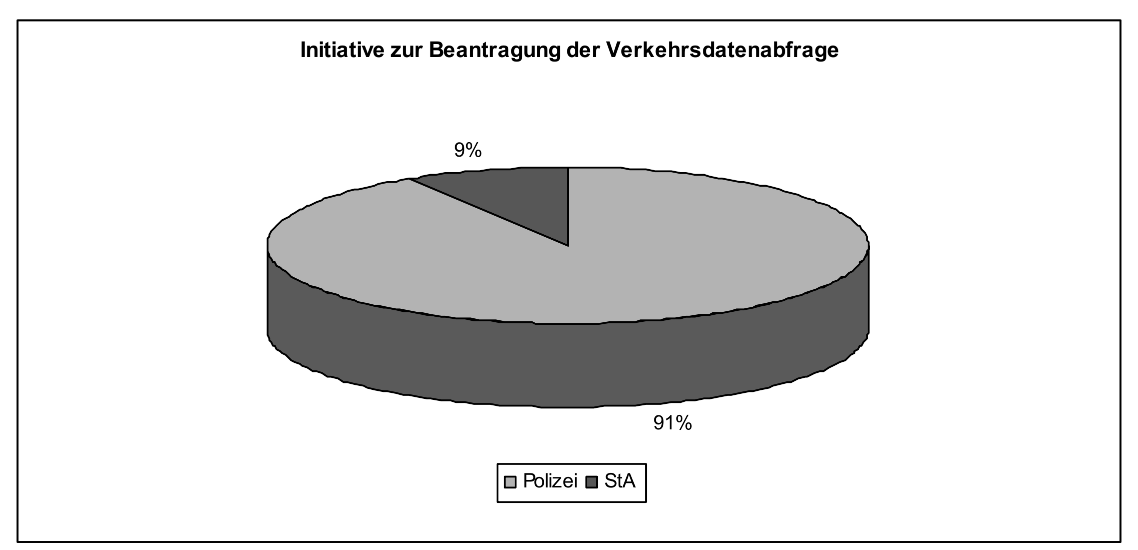


Abbildung 34

Dauer von Anregung bis Antrag

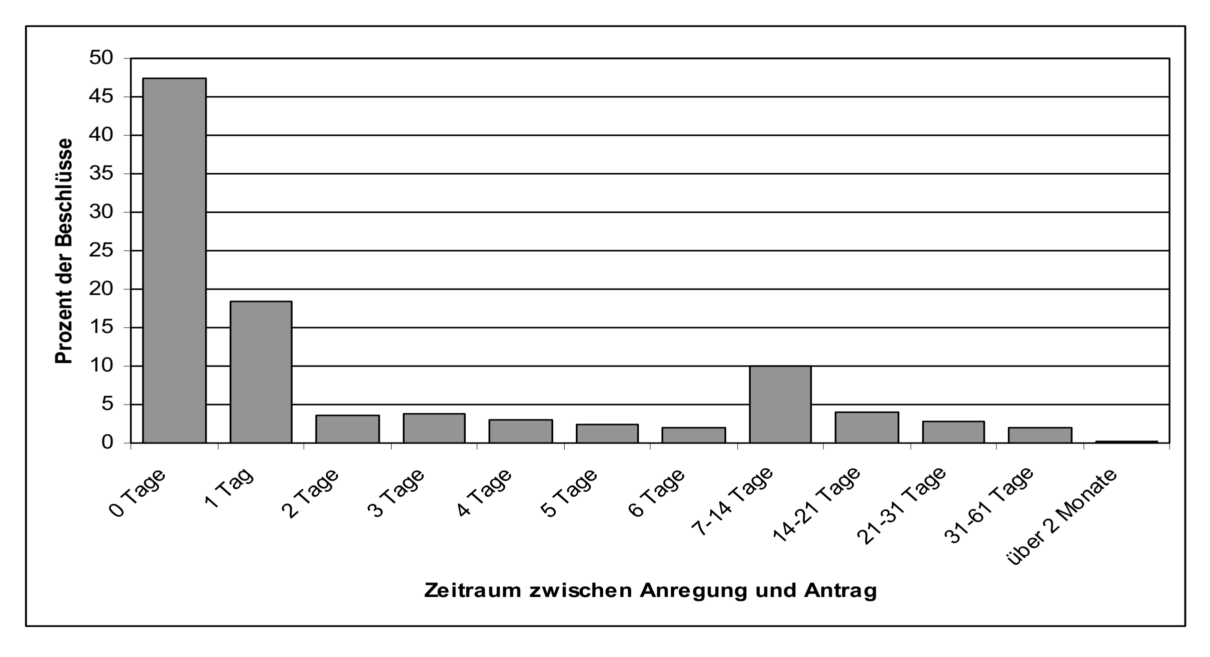


Abbildung 35

Dauer von Antrag bis Beschlusserlass

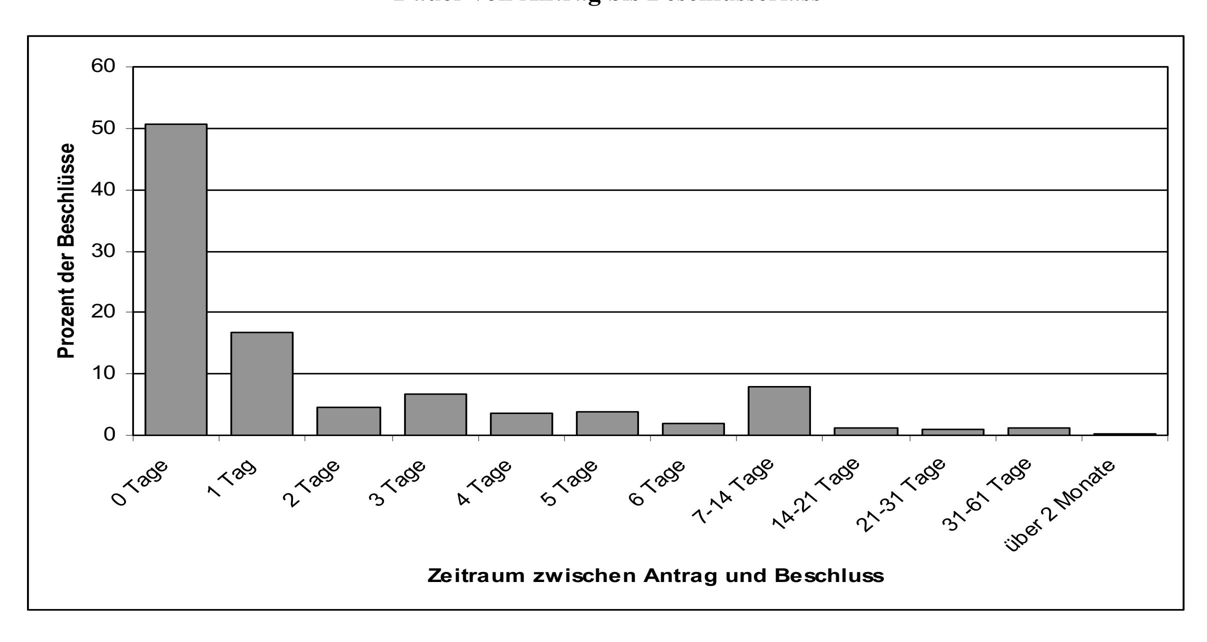
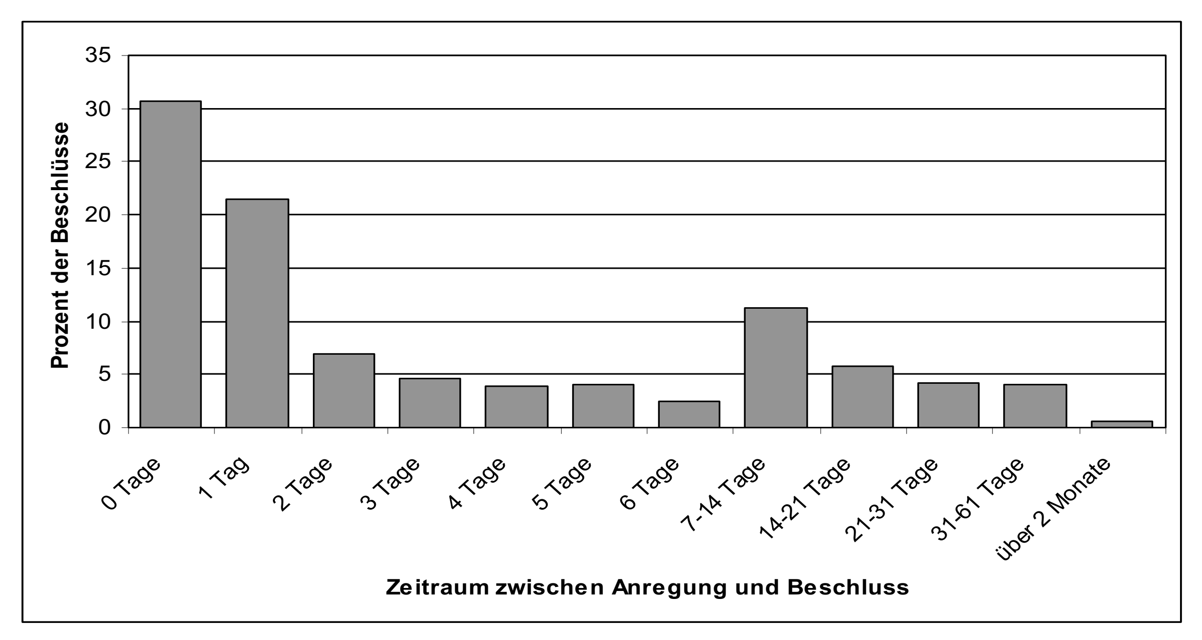


Abbildung 36

Dauer von Anregung bis Beschlusserlass



3. Experteninterviews

a) Polizeibeamte

(1) Geschäftsablauf

Die Beantragung von §§ 100gh-Maßnahmen wird in den Dienststellen aller befragten Polizeibeamten durch die jeweiligen Sachbearbeiter bzw. die jeweilige ermittlungsführende Stelle vorgenommen. Die befragten Polizeibeamten gaben überwiegend an, dass es eine spezielle Abteilung gebe, welche die Verkehrsdatenabfrage abwickelt. Dabei werden regionale Unterschiede erkennbar. Diese Servicedienststellen gibt es in Berlin, Mecklenburg-Vorpommern und Nordrhein-Westfalen, in Baden-Württemberg dagegen nicht. In Mecklenburg-Vorpommern ist für die Erhebung der Verkehrsdaten eine spezielle Abteilung im Landeskriminalamt zuständig, während die Durchführung der Telekommunikationsüberwachungsmaßnahmen durch die jeweiligen Dienststellen erfolgt. Zwei der Sachbearbeiter aus einer solchen Abteilung wurden von uns befragt. In diesen zentralen Dienststellen werden Telekommunikationsüberwachungen, Verkehrsdatenabfragen und Anschlussinhaberfeststellungen koordiniert und ausgewertet. Diese Anlaufstellen beraten die anfragenden Dienstellen über die möglichen Ermittlungsmaßnahmen, die rechtlichen und praktischen Möglichkeiten, und setzen sich zur Umsetzung der Beschlüsse mit den Netzbetreibern in Verbindung. Nur über diese Dienstellen findet der Kontakt zu den Netzbetreibern statt. Von diesen Abteilungen werden die Daten auch analysiert und bewertet und das Ermittlungsergebnis an die jeweilige Dienststelle übermittelt.

Hinsichtlich der technischen Möglichkeiten wurden vier der Befragten besonders geschult. Dabei wurden u. a. Informationsveranstaltungen des Spezialdezernats als Schulungsform genannt. Weiter wurde angegeben, dass die Kollegen in der Spezialabteilung besonders geschult seien. Zwei der Befragten gaben an, dass ihre Kenntnisse auf Erfahrungswissen beruhen. Erst in der Praxis würde man erkennen, „was wirklich möglich ist und was die Maßnahme bringt“. Weitere Informationsquellen seien schriftliche Merkblätter, regelmäßige Besprechungen, auf denen Neuerungen mitgeteilt werden, und Beiträge in Fachzeitschriften. Zudem gebe es allgemeine Lehrgänge zu den Ermittlungsmethoden sowie Fortbildungen. Von zwei weiteren Befragten wurde kritisch angemerkt, dass die Verkehrsdatenabfrage dabei nur am Rande angesprochen würde. Weiter wurden Lehrgänge zur Telekommunikationsüberwachung und Computerkriminalität genannt, bei denen rechtliche, technische und taktische Fragen behandelt würden.

Ein Mitarbeiter aus den Telekommunikationsüberwachungsspezialstellen gab an, dass es speziell für ihre Abteilung umfangreiche Schulungen gebe. Es handle sich um einen sehr schnelllebigen Bereich, was Erhebungsmöglichkeiten, Inhalt und Bewertung angingen. Regelmäßige Schulungen seien daher unerlässlich. Das Rahmenwissen werde an die Abteilungen weitergegeben. Über technische Fragestellungen hinaus, sei auch eine Schulung in Rechtsfragen sinnvoll.

Der Geschäftsablauf wird von allen befragten Polizeibeamten ähnlich geschildert. Wenn sich die Maßnahme anbietet, erforderlich ist und die Voraussetzungen vorliegen, regt der Sachbearbeiter die Maßnahme bei der Staats-

anwaltschaft an, die den Beschluss beim Gericht beantragt. Die Anregung erfolge in (persönlicher oder telefonischer) Absprache mit der Staatsanwaltschaft. Das Gericht erlässt den Beschluss und sendet ihn an die Staatsanwaltschaft oder direkt an die Polizei bzw. das Landeskriminalamt. Von der Polizei (ggf. von der Spezialdienststelle) aus wird der Beschluss dann (per Fax) an die Netzbetreiber weitergeleitet und die Daten werden direkt an die Polizei zurückgeschickt. Das Verfahren wurde mehrfach als „Geschäftsgang mit kurzen Wegen" beschrieben. Es komme durchaus vor, dass die Polizei den Beschluss selbst beim Gericht abholt. Gerade in Eilfällen gehe die Polizei persönlich mit der Akte zur Staatsanwaltschaft und dann weiter zum Gericht. Die Daten werden von den Providern per Diskette, CD oder Fax geliefert. Teilweise wurde angegeben, dass die Provider ausdrücklich darum gebeten werden, die Daten in elektronischer Form zu übersenden. Denn wenn die Daten in Papierform geschickt werden, müssen sie erst aufwändig in eine Excel-Tabelle eingegeben werden. Der Vorteil der zentralen Stelle, die die Maßnahmen umsetzt, wird darin gesehen, dass die Provider einen zentralen Ansprechpartner haben. Zudem erfolgt auch die operative Auswertung durch diese Abteilungen.

(2) Besprechungen

Nach Angabe der Befragten erfolgen vor Anregung der §§ 100g, 100h-Maßnahme in der Regel Besprechungen mit der Staatsanwaltschaft. Dabei werde die Notwendigkeit der Maßnahme dargelegt. Von der Anregung einer Maßnahme werde von vornherein abgesehen, wenn erkennbar sei, dass der Staatsanwalt ihr ablehnend gegenübersteht. Die Besprechung diene somit der Klärung, ob der Staatsanwalt den Antrag mitträgt. Die Polizei lässt sich den Antrag also bereits vor der schriftlichen Anregung „absegnen". Besprochen werde auch, wie das Verfahren weiter betrieben werden solle. Gerade bei komplexen Fällen würden die Maßnahmen und das Vorliegen der rechtlichen Voraussetzungen auf diese Weise besprochen. Mitunter sei es auch vorgekommen, dass der Staatsanwalt die Abfrage der Verkehrsdaten anrege. Drei der Befragten gaben an, dass die Besprechung mit der Staatsanwaltschaft nicht die Regel sei, aber im Einzelfall bzw. in Grenzfällen vorkomme. Dies hinge jeweils von der Bedeutung des Verfahrens ab. Nur wenn die Erforderlichkeit offenkundig sei, würde der Beschluss ohne Besprechung angeregt. Auch bei Eilfällen würde die Staatsanwaltschaft vorher informiert. Die meisten der Polizeibeamten gaben an, dass mit Richtern im Vorfeld der Beantragung keine Absprachen getroffen werden. Nach ihrer Erfahrung gebe es nur im Einzelfall Nachfragen vom Gericht. Als konkretes Beispiel wurde angeführt, dass Richter nachhaken, welche Anhaltpunkte dafür vorliegen, dass Telekommunikation eine Rolle gespielt hat. Dann werde mit gleichgelagerten Fällen, also mit der Tatphänomenologie, argumentiert. Die Staatsanwaltschaft sei als Zwischeninstanz vorgegeben. Mitunter wurde auch darauf verwiesen, dass der Staatsanwalt die Richter häufig kenne und wisse, ob die Begründung ausreiche. Eine Person äußerte explizit, ihr sei kein einziger Fall bekannt, in dem jemals ein Antrag von Gerichtsseite abgelehnt worden wäre. Entweder stelle der Staatsanwalt den Antrag gar nicht erst, wenn er wisse, dass er nicht bewilligt werde, oder er stelle ihn in der Gewissheit, dass der Beschluss wie beantragt erlassen werde.

(3) Datensicherung

Die Frage, ob bei den Telekommunikationsanbietern nachgefragt wird, ob die Daten noch gespeichert sind, wird von den meisten Polizeibeamten mit der Begründung verneint, dass die Speicherfristen der Netzbetreiber bekannt seien. Vereinzelt wurde angegeben, dass Nachfragen im Einzelfall erfolgen. Sie begründeten dies mit der unterschiedlichen Speicherdauer und den häufigen Änderungen. Die Speicherfristen der großen Anbieter seien zwar bekannt, nicht jedoch die der kleineren Unternehmen. Einige Befragte gaben an, dass um Datensicherung nur ausnahmsweise, etwa bei Fristproblemen, gebeten werde. Andere dagegen meinten, dass sie um Datensicherung bitten. Die Daten würden dann zunächst beim Anbieter eingefroren, darauf hin der Beschluss erwirkt und daraufhin die Daten herausgegeben. Ein Befragter stand der Datensicherung sehr skeptisch gegenüber. Denn wenn die Beschlüsse dann doch nicht erlassen werden, bleiben die Anbieter „auf den Kosten sitzen". Deswegen weigerten sich die Anbieter mitunter, Daten auf Verlangen einzufrieren. Hierzu passt auch die Erfahrung eines anderen Befragten, der berichtete, dass die Daten von den Anbietern erst nach Vorlage eines Beschlusses eingefroren würden. Der Verdacht verfestige sich erst im Laufe der Zeit. Ein Einfrieren der Daten bis zur Verdachtserhärtung gegen den Beschuldigten sei daher sinnvoll. Denn erst dann könne ein Beschluss erwirkt werden. Es sei wünschenswert, dass eine gesetzliche Regelung geschaffen werde, die festlege, dass die Daten bei schwerwiegenden Delikten eingefroren werden können.

(4) Bereitschaft zum Einsatz der Maßnahmen

Die Bereitschaft zum Einsatz der Maßnahmen bei Polizei, Staatsanwaltschaft und Gericht wird von den befragten Polizeibeamten unterschiedlich eingeschätzt. Die Hälfte der Befragten gab an, dass die Bereitschaft generell sehr groß sei. Es sei eine Standardmaßnahme geworden, die den Betroffenen nicht so stark belaste wie beispielsweise eine DNA-Analyse oder eine erkennungsdienstliche Behandlung. Einige andere verwiesen hingegen darauf, dass abgewogen werde, ob die Maßnahme tatsächlich durchgeführt werden soll, denn man müsse mit den Konsequenzen leben. Gerade bei Funkzellenabfragen würden die Datenmassen einen großen Arbeitsaufwand bedeuten. Die Staatsanwaltschaft käme den Anregungen zumindest bei Betäubungsmitteldelikten immer nach. Die Bereitschaft der Strafverfolgungsbehörden sei von der Effizienz der Maßnahme abhängig, meint einer der anderen Befragten. Man greife eher zu einem Instrumentarium, wenn man damit bereits Erfolge erzielen konnte. Die Maßnahme müsse sich in dem jeweiligen Fall anbieten. Man versuche, die rechtlichen Möglichkeiten auszuschöpfen. Es sei eine Maßnahme, die sich als feste Möglichkeit eta-

bliert habe und zum festen Bestand gehöre. Sie würde immer in Betracht gezogen und geprüft, ob mit ihr in einem konkreten Fall etwas erreicht werden könne.

b) Staatsanwälte

(1) Geschäftsablauf

Den Geschäftsablauf nach Anregung einer Maßnahme nach §§ 100g, 100h StPO schildern fast alle befragten Staatsanwälte gleich. Die Polizei rege die Maßnahme an. Dann prüfe die Staatsanwaltschaft, ob die Voraussetzungen vorliegen, und beantrage die Maßnahme beim Ermittlungsrichter. Der Richter erlasse den Beschluss. Akte und Beschluss würden zurück an die Staatsanwaltschaft gehen und von dort an die Polizei. Die Polizei sei es dann in der Regel, die die Ausfertigungen an die Provider sende. Ein Befragter meint, dass die Staatsanwaltschaft die Daten direkt bei den Telekommunikationsunternehmen anfordere. Im Eilfall komme die Polizei persönlich vorbei und rege die Maßnahme an. Ebenso würden im Eilfall die Akte und der Beschluss direkt wieder beim Gericht von der Polizei abgeholt bzw. der Beschluss der Polizei zugefaxt oder der Beschluss gehe per Fax oder im Original an die Unternehmen.

(2) Besprechungen

Die meisten befragten Staatsanwälte berichten übereinstimmend, dass vor der Antragstellung meist Besprechungen mit der Polizei stattfinden. Die Polizei erkläre die Umstände und es würde darüber gesprochen, ob die Voraussetzungen für die Maßnahme vorliegen. Einige Befragte meinen, dass die Abstimmung mit der Polizei zumindest bei größeren Sachen die Regel sei. Man überlege dann gemeinsam, wie weiter vorgegangen werden solle und welche Ermittlungsansätze sich anböten. In einigen Dienststellen erfolgt die Rücksprache mit der Polizei nur in Einzelfällen bzw. Ausnahmefällen. Im Übrigen komme es vor, dass die die Polizei in Eilfällen vorher anrufe und eine Besprechung stattfände. Ein Staatsanwalt meinte, dass die Initiative zur Maßnahme teilweise auch von ihm ausgehe, wenn er sie für sinnvoll hält. Vorherige Besprechungen mit dem Gericht finden hingegen seltener statt oder sind gar die Ausnahme. Nur wenn dem Antrag nicht gefolgt werden soll oder der Richter Nachfragen habe, käme es zu einem Gespräch zwischen Polizei und Gericht. Ein Staatsanwalt erläuterte, dass die Richter i. d. R. wissen würden, dass Anträge ausreichend geprüft werden. Bei Schwierigkeiten oder Zweifeln rufe die Staatsanwaltschaft den Richter vorher an, was aber sehr selten sei. Bei Eilfällen würden die Richter häufiger telefonisch vor Beantragung der Maßnahme informiert. Nach den Angaben von weiteren Befragten finden Besprechungen im Vorfeld der Beantragung der Maßnahme mit der Polizei oder dem Gericht in der Regel nicht statt. Es müsste sich alles aus der Akte ergeben.

(3) Bereitschaft zum Einsatz der Maßnahmen

Die Bereitschaft zum Einsatz der Maßnahmen nach §§ 100g, 100h StPO wird von einem Befragten uneingeschränkt als hoch einschätzt. Ein Befragter erklärt, die Bereitschaft der Polizei sei gestiegen. Die Verkehrsdatenabfrage habe sich gut etabliert. Ein anderer Befragter gibt an, dass die Verkehrsdatenabfrage gegenüber einer Telefonüberwachung eher angeordnet werde, weil die Anforderungen an den Beschlusserlass niedriger seien. Je niedriger die Anforderungen an den Erlass, desto eher bediene man sich der Methode. Weiter wurde ausgeführt, dass die Bereitschaft grundsätzlich vorhanden sei, es sich aber um eine arbeitsintensive Maßnahme handle. Deshalb werde eher zurückhaltend davon Gebrauch gemacht. Die geringere Eingriffsintensität erhöhe die Bereitschaft im Vergleich zu Maßnahmen nach §§ 100a, 100c, 163f I StPO. Die Bereitschaft zu § 100g StPO sei jedoch geringer als bei der Durchsuchung. Einige der Befragten meinen, die Bereitschaft hänge vom Einzelfall ab. Wenn es eine andere effektive Möglichkeit gebe, werde man diese ergreifen. In Bezug auf die Bereitschaft gebe es keinen Unterschied zu anderen Maßnahmen. Die Bereitschaft zur Durchführung der Maßnahme sei bei den Ermittlungsbehörden und dem Gericht vorhanden, wenn der Einsatz der Maßnahme erforderlich ist. Soweit keine anderen Ermittlungsansätze vorhanden seien, seien die Maßnahmen ein probates Mittel und würden in letzter Zeit zunehmend eingesetzt.

c) Richter

(1) Geschäftsablauf

Alle befragten Ermittlungsrichter schilderten den Geschäftsablauf gleichermaßen. Die Polizei rege die Maßnahme an und die Staatsanwaltschaft stelle einen Antrag. Die Akte mit dem Antrag gehe von der Staatsanwaltschaft an die Geschäftsstelle des Gerichts, wo der Maßnahme ein Gs-Aktenzeichen zugeteilt werde. Die Staatsanwaltschaft gebe in dem Antrag vor, welche Maßnahme und welchen zeitlichen Rahmen sie sich vorstelle. Der Richter prüfe dann, ob die Voraussetzungen vorliegen und treffe seine Entscheidung. Der Beschluss werde entweder über die Staatsanwaltschaft oder direkt an die Polizei geschickt; diese versende ihn dann an die Netzbetreiber. Auch die Auskunft gehe dann wieder an die Polizei oder die Staatsanwaltschaft. Von einem Befragten wurde angegeben, dass dieser Vorgang bis zu 14 Tagen dauere. Anders verhalte es sich bei Eilbedürftigkeit. Die Polizei komme dann mit der Akte und dem Antrag der Staatsanwaltschaft persönlich zum Gericht und nehme die Akte und den Beschluss nach der Prüfung wieder mit

(2) Besprechungen

Auch von Richterseite wird die Besprechungspraxis unterschiedlich beschrieben. Nach Angabe einiger Richter finden Besprechungen mit der Polizei oder der Staatsanwaltschaft vor Erlass des Beschlusses nach §§ 100g, 100h StPO nie statt. Einige andere bezeichneten solche als selten und wiederum andere gaben an, dass dies teilweise vorkomme (z. B. bei Verlängerungsanträgen). Dass Polizei oder Staatsanwaltschaft vorab anfragen, ob ein Antrag erfolgversprechend sei, wird eher als selten bezeichnet. Besprechungen gebe es eher, wenn es um die Nachbesse-

rung von Anträgen oder um Rückfragen zu Akten gehe. Dann würden sie sich an die Staatsanwaltschaft wenden und diese würde ggf. weitervermitteln zur Polizei. Sie würden dann um Überarbeitung des Antrags bitten bevor der Antrag abgelehnt werde. Ein Befragter führte aus, dass er auch dann telefonisch Rücksprache halte, wenn er eine andere Art der Maßnahme (als z. B. eine Funkzellenabfrage) für angemessen halte. Auch bei Folgebeschlüssen würden kurze Besprechungen geführt, so dass die Akte nicht erneut geschickt und keine langen Begründungen abgegeben werden müssten.

(3) Bereitschaft zum Einsatz der Maßnahmen

Auch auf Richterseite wird die Bereitschaft zum Einsatz der Maßnahmen bei Polizei, Staatsanwaltschaft und Gericht teilweise als hoch eingeschätzt. Es werde vermehrt und schnell davon Gebrauch gemacht. Es sei beispielsweise einfacher, zunächst Verkehrsdaten abzufragen, als direkt eine Durchsuchung der Wohnung anzuordnen. Das sei auch eine Frage der Verhältnismäßigkeit. Der Vorgang habe sich eingespielt und sei zum Routinevorgang geworden. Teilweise wurde angegeben, dass die Polizei eine sehr hohe Bereitschaft zur Anwendung der Maßnahme habe. Ein Befragter meint, die Polizei sei „ganz begeistert“ davon und die Staatsanwaltschaft folge ihr dabei. Dazu wurde angemerkt, dass die Polizei allgemein sehr bestrebt zum Einsatz von Maßnahmen sei, dies aber nicht stärker bei der Verkehrsdatenabfrage sei als bei anderen Methoden. Die Filterfunktion der Staatsanwaltschaft gewährleiste, dass viele Anträge bzw. Anregungen gar nicht erst an das Gericht weitergegeben würden. Bei der Staatsanwaltschaft entstehe nicht der Eindruck, dass sie oft darauf zurückgreife. Sie bremse die Polizei teilweise. Die Maßnahme gehöre schon zu den häufigeren Ermittlungsmethoden, sei fast zum Standard geworden. Aber man könne daraus keine Rückschlüsse auf die Bereitschaft ziehen. „Wenn die Ermittlungsbehörden die Möglichkeit haben, greifen sie auch danach“, sagt ein Richter, verweist aber zugleich darauf, dass die Polizei sich sonst aber auch vorwerfen lassen müsse, warum sie die Möglichkeit nicht genutzt habe.

d) Verteidiger

Die Bereitschaft zum Einsatz der Maßnahmen bei Polizei und Justiz wird von den meisten befragten Anwälten als hoch eingeschätzt. Die Hemmschwelle, die Maßnahme anzuwenden, sinke. Von einem Befragten wird insbesondere die Bereitschaft der Polizei als sehr hoch eingeschätzt. Die Maßnahme sei auch deshalb sehr beliebt, weil es die Ermittlungsbehörden wenig koste und einfach umzusetzen sei. Es sei mittlerweile eine Standardmaßnahme geworden.

e) Telekommunikationsunternehmen

(1) Aufforderung zur Datensicherung

Ob ihr Unternehmen vor Erlass des Beschlusses bzw. der Eilanordnung zur längeren Speicherung der Daten durch die Polizei aufgefordert werde, beantworteten die Unternehmen unterschiedlich. Die Befragten aus drei Unternehmen gaben an, dass sie von Polizei und Staatsanwaltschaft gelegentlich um dieses „Quick-freeze“-Verfahren (oder „Fast-freeze“) gebeten würden, sich aber nicht darauf einließen. Der Gesetzgeber habe sich bisher dagegen entschieden, die Daten länger zu speichern. Die Speicherung sei kundenabhängig. Jeder Kunde entscheide selbst, wie lange seine Daten gespeichert werden sollen. Die Mitarbeiter von zwei anderen Unternehmen gaben an, dass dies häufig sei bzw. immer wieder versucht werde, vor allem durch die Polizei, aber teilweise auch von der Staatsanwaltschaft oder vom Gericht. Sie würden dies aber ablehnen, da es dafür keine Rechtsgrundlage gebe. Sie würden sich nach § 206 StGB strafbar machen, meint einer der Befragten. Lediglich in einem der in die Befragung einbezogenen Unternehmen ist man in der Regel nicht mit dieser Problematik konfrontiert.

(2) Anfragen zur Speicherung

Alle Anbieter geben an, dass es vorgekommen sei, dass die Polizei im Vorfeld einer Anordnung angefragt hätte, ob die Daten noch gespeichert sind. Auch Anfragen anderer Art kommen vor. Nur hinsichtlich der Häufigkeit variieren die Antworten. Ein Befragter meint, dies sei regelmäßig der Fall (zwei- bis fünfmal täglich). Es würden aber nur allgemeine Auskünfte über die Speicherdauer gegeben, aber nicht darüber, ob eine Person telefoniert habe. Denn unter das nach § 88 TKG zu beachtende Fernmeldegeheimnis falle bereits die Information, ob jemand an Telekommunikation teilgenommen hat. Zwei andere Befragte kritisieren dies und erklären, dass sie in diesen Fällen auf die rechtlichen Voraussetzungen verweisen. Andere Unternehmen hingegen erteilen die begehrte Auskunft, ob die Daten noch gespeichert sind oder nicht. Auch technische Anfragen seien recht häufig. Einer dieser Befragten erläutert, dass für Fragen eine Hotline eingerichtet sei, für die es zwar keine rechtliche Verpflichtung, aber offensichtlichen Bedarf gebe. Es würden informatorische Befragungen stattfinden. Es werde aber z. B. nicht darüber Auskunft erteilt, wenn nach bestimmten Rufnummern und ähnlichen in die Tiefe gehenden Informationen gefragt werde. Dafür bedürfe es eines Beschlusses.

4. Zusammenfassung der Ergebnisse

Sowohl aus den Ergebnissen der schriftlichen Befragung als auch aus der Aktenanalyse ergibt sich, dass die Initiative zur Beantragung einer Maßnahme nach §§ 100g, 100h StPO größtenteils von der Polizei ausgeht. 73 Prozent der schriftlich befragten Staatsanwälte schätzten, dass die Polizei in 80 bis zu 100 Prozent aller Fälle Initiator für die Durchführung der Verkehrsdatenabfrage ist. Bestätigt und sogar noch verstärkt wurde dieses Ergebnis durch die Auswertung der Verfahrensakten. Danach initiierte die Polizei in 91 Prozent der Fälle die Beantragung der Maßnahme, während die Staatsanwaltschaft nur in 9 Prozent der Fälle eine solche Maßnahme von sich aus anregte. Auch aus den Expertengesprächen folgt, dass die Staatsanwälte nur ab und zu selbst die

Durchführung einer solchen Maßnahme initiieren. Allerdings ist zu berücksichtigen, dass im Vorfeld der Beantragung nach den Ergebnissen der Aktenanalyse und den Expertengesprächen teilweise Besprechungen vor allem zwischen Polizei und Staatsanwaltschaft stattfinden. Bei 8 Prozent der Beschlüsse wurden solche Besprechungen ausdrücklich in den Akten vermerkt, wobei zu vermuten ist, dass dies in weiteren Fällen vorgekommen und nicht vermerkt worden ist. Auch aus den Expertengesprächen mit den Polizeibeamten und Staatsanwälten zeigt sich, dass in der Regel vor Anregung einer Maßnahme nach §§ 100g, 100h StPO besprochen wird, ob eine solche Maßnahme beantragt werden soll oder nicht. Die Polizei legt den Sachverhalt dar und gemeinsam wird beraten, ob die Verkehrsdatenabfrage die geeignete und notwendige Ermittlungsmaßnahme wäre. Besprechungen zwischen Polizeibeamten bzw. Staatsanwalt und Richter kommen dagegen selten vor. Sowohl aus der Auswertung der Verfahrensakten als auch aus den Interviews geht hervor, dass es sich in solchen Fällen um Rückfragen des Richters oder Korrekturen des Antrags handelt.

Der Ablauf von der Anregung der Maßnahme bis zur Anordnung der Maßnahme, der in den Akten ersichtlich ist, wird durch die interviewten Experten bestätigt. Die Polizei regt die Maßnahme grundsätzlich bei der Staatsanwaltschaft an. Die Staatsanwaltschaft stellt beim Gericht einen Antrag auf Durchführung einer Verkehrsdatenabfrage und der Ermittlungsrichter erlässt den Beschluss. Vom zeitlichen Ablauf her erfolgt – wie sich aus den Ergebnissen der Aktenanalyse ergibt – dieser Vorgang zumeist innerhalb von sechs Tagen (74 Prozent). Der Beschluss wird meist über die Polizei zu den verpflichteten Netzbetreibern geschickt und die Ergebnisse werden von diesen auch direkt an die Polizei geliefert. Bei der Polizei erfolgt die Anforderung der Daten bei den Diensteanbietern und die Auswertung der Daten (abgesehen von Baden-Württemberg) meist in speziellen Dienststellen mit geschultem Personal. Die Hälfte der Polizeibeamten bestätigte die Aussage der Telekommunikationsanbieter, dass vor Beschlusserlass teilweise um Datensicherung gebeten wird. Die Anbieter gaben zudem an, dass es teilweise vorkomme, dass die Polizei bei ihnen nachfrage, ob die Daten überhaupt noch gespeichert sind. Die Einrichtung einer Hotline zur Beratung über die technischen Möglichkeiten der Abfrage macht noch deutlicher, in welchem Umfang die Telekommunikationsanbieter über die Umsetzung der Beschlüsse hinaus in die Ermittlungstätigkeit involviert sind.

Die Bereitschaft zum Einsatz der Verkehrsdatenabfrage wird von den befragten Experten unterschiedlich beurteilt. Teilweise wurde angegeben, dass die Bereitschaft genauso groß sei wie bei anderen Ermittlungsmaßnahmen. Teilweise wird die Bereitschaft zum Einsatz der Verkehrsdatenabfrage allgemein als groß angesehen, da sie sich als Standardmaßnahme etabliert habe. Zum Teil wird – gerade von Ermittlungsrichtern – die Bereitschaft bei der Polizei als höher eingeschätzt als bei Staatsanwaltschaft und Gericht. Auch die interviewten Verteidiger titulierten die Verkehrsdatenabfrage als Standardmaßnahme.

III. Anordnung der Verkehrsdatenabfrage und Begründungen

Im Folgenden wird dargestellt, in welchem Umfang Gericht und Staatsanwaltschaft Anordnungen erlassen und welche Qualität Anregung, Antrag und Beschluss aufweisen.

1. Schriftliche Befragung

a) Anteile der richterlichen und staatsanwaltschaftlichen Anordnungen

Auf die Frage, wie sie den Anteil an gerichtlichen Anordnungen einschätzen, antworteten 686 (78 Prozent) der Befragten im Hinblick auf ihre eigene Erfahrung, 553 (63 Prozent) in Bezug auf ihre Abteilung und 508 (58 Prozent) auch in Bezug auf die gesamte Behörde. Die Verteilung der Antworten ist in Abbildung 37 dargestellt. Im Mittel wurde aufgrund der Eigenerfahrung geschätzt, dass 87 Prozent der Anordnungen durch einen Richter erfolgen. Dieser Prozentsatz reduziert sich geringfügig für die Schätzungen bzgl. der Abteilungen auf 86 Prozent und für die Behörde auf 83 Prozent.

Bei den Schätzungen sind keine signifikanten Unterschiede im Rahmen der Dezernatszugehörigkeit der Staatsanwälte zu bemerken, was die Abteilung oder Behörde insgesamt betrifft. An der Grenze zu Signifikanz bewegen sich diesbezüglich lediglich die Schätzungen auf der Basis der eigenen Erfahrung.

Je nach Bundesland, in dem die befragten Staatsanwälte arbeiten, gibt es bei den Schätzungen bzgl. des Anteils der gerichtlichen Beschlüsse signifikante Unterschiede. Wie Abbildung 38 zeigt, treten Thüringen, Schleswig-Holstein und Hessen durch die geringe Häufigkeit der richterlichen Anordnungen hervor.

Im Gegensatz zur allgemeinen Tendenz, dass die Häufigkeit der richterlichen Anordnung aus eigener Erfahrung höher eingeschätzt wird als die für die Abteilung oder sogar für die gesamte Behörde, sind bei Schleswig-Holstein, Sachsen-Anhalt und Hessen diesbezüglich andere Reihenfolgen auffällig.

Von den 874 Befragten beantworteten 697 die Frage, ob nach ihren Erfahrungen der Anteil der staatsanwaltschaftlichen Anordnungen im Vergleich zum Vorjahr anstieg. Von diesen gaben 61 Prozent an, dass keine Veränderung zum Vorjahr festzustellen sei. 12 Prozent konstatierten einen Anstieg, 6 Prozent einen Rückgang der Eilanordnungen.

588 der Befragten machten auch Angaben dazu, wie schnell eine Eilanordnung vom Richter bestätigt wird. 57 Prozent gaben an, dass dies am nächsten Tag erfolgen würde. 25 Prozent nannten den übernächsten Tag nach der Eilanordnung, 16 Prozent gaben den dritten Tag nach der Eilanordnung als Antwort an und 3 Prozent nannten den Tag der Eilanordnung selbst.

Abbildung 37

Einschätzung der Anteile richterlicher Anordnungen

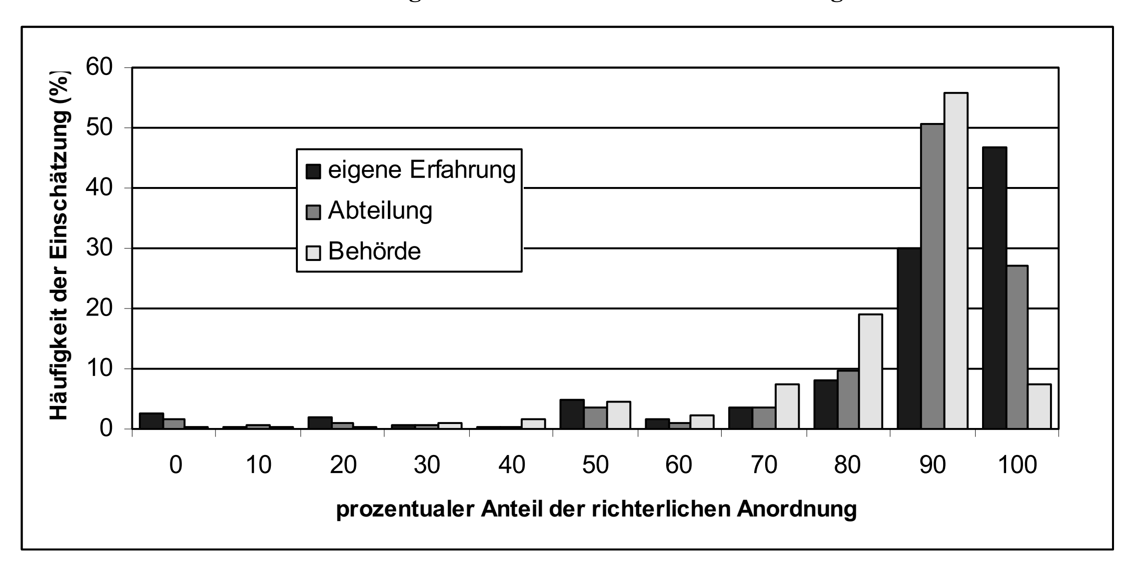
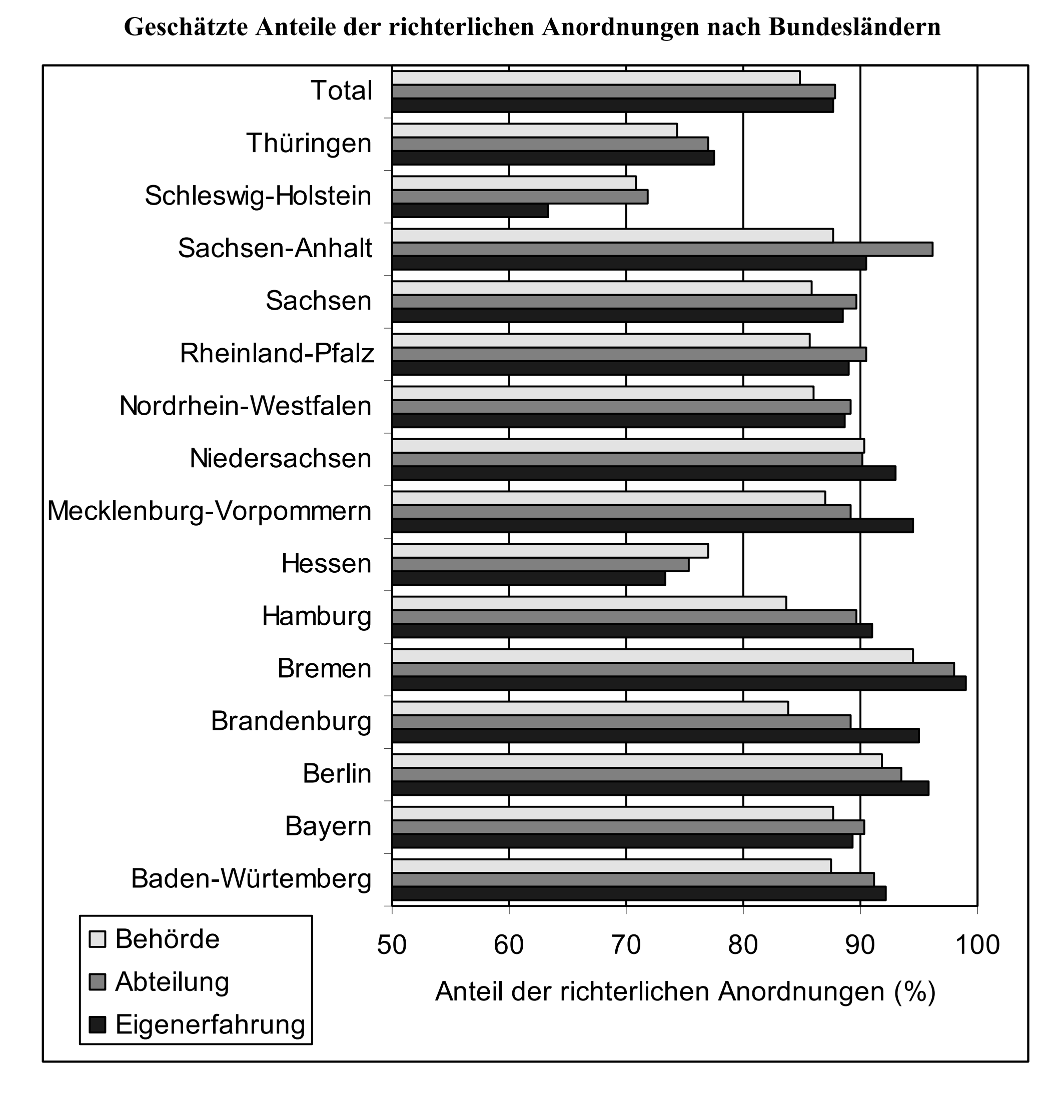


Abbildung 38

Geschätzte Anteile der richterlichen Anordnungen nach Bundesländern



b) Richtervorbehalt

Ganz generell halten 62 Prozent der Befragten den Richtervorbehalt für (eher) sinnvoll. 28 Prozent halten den Richtervorbehalt eher nicht für sinnvoll und 10 Prozent schätzen ihn als sinnlos ein.

Dementsprechend waren 61 Prozent dafür, den Richtervorbehalt unverändert beizubehalten (siehe Abbildung 39). 38 Prozent sind der Ansicht, dass der Richtervorbehalt eingeschränkt werden sollte. Demgegenüber forderte lediglich ein knappes Prozent die Erweiterung des Richtervorbehalts.

c) Ablehnung von Anträgen

Die Befragten gaben an, dass Anträge nie (30 Prozent) bzw. selten (58 Prozent) abgelehnt wurden. 11 Prozent sprachen davon, dass Anträge gelegentlich vom Richter abgelehnt werden. Wie diese Ablehnung nach Erfahrung der Befragten im Einzelnen begründet wird, ist in Abbildung 40 dargestellt. Als häufigster Ablehnungsgrund wird die Verneinung einer Straftat von erheblicher Bedeutung genannt. Fast genauso häufig werden nach den Erfahrungen der Befragten Anträge mit der Begründung abgelehnt, dass kein hinreichender Tatverdacht besteht. Deutlich seltener sind nach Angabe der Befragten Ablehnungen der Maßnahmen aus dem Grund, dass ein milderes Mittel in Betracht kommt oder die Maßnahme keinen Erfolg verspricht. Als sonstige Begründungen wurden (örtliche) Unzuständigkeit oder ein ungenauer Antrag genannt. Angegeben wurde auch, dass keine Anhaltspunkte dafür vorlagen, ob tatsächlich Telekommunikationseinrichtungen genutzt wurden.

d) Bestätigung von Eilanordnungen

Staatsanwaltschaftliche Eilanordnungen werden nach Einschätzung der Befragten immer (60 Prozent) oder häufig (38 Prozent) bestätigt. Nur 2 Prozent gaben an, dass eine Bestätigung gelegentlich, selten oder nie erfolge. Informelle Ablehnungen durch Vorgespräche mit dem Richter erfolgten nach Angabe der Befragten nie (47 Prozent) bis selten (42 Prozent). Nur 10 Prozent sprachen hier von gelegentlichen Ablehnungen in dieser Form. 1 Prozent meinen, dass solche Ablehnungen häufig oder immer stattfinden.

Abbildung 39

Beibehaltung des Richtervorbehalts

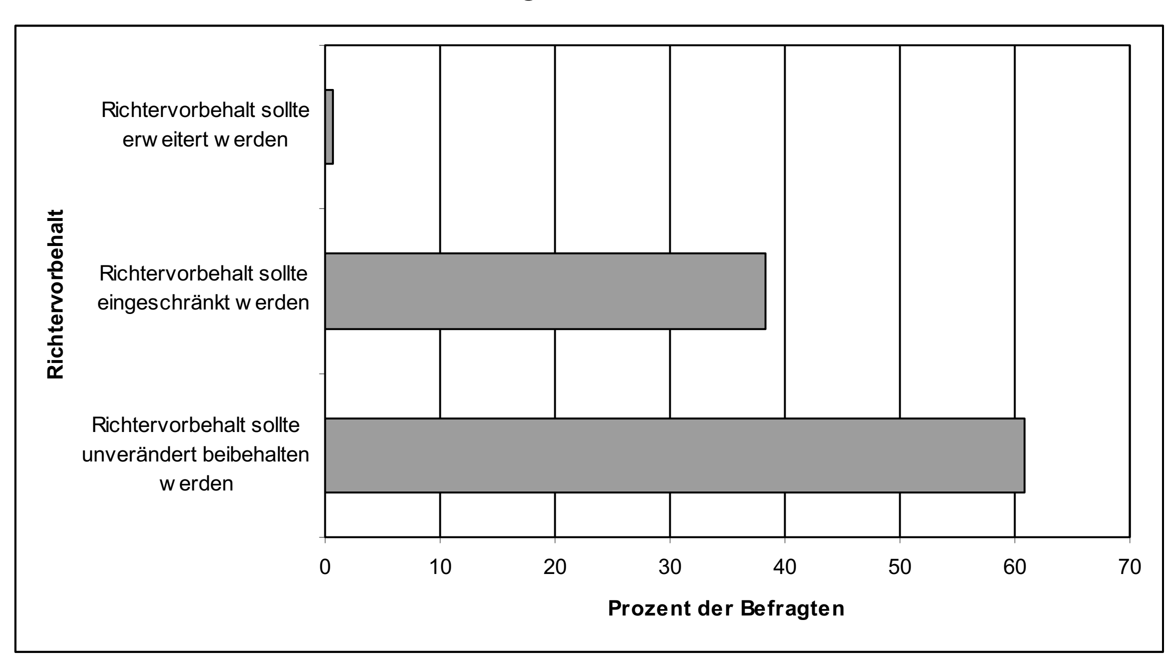
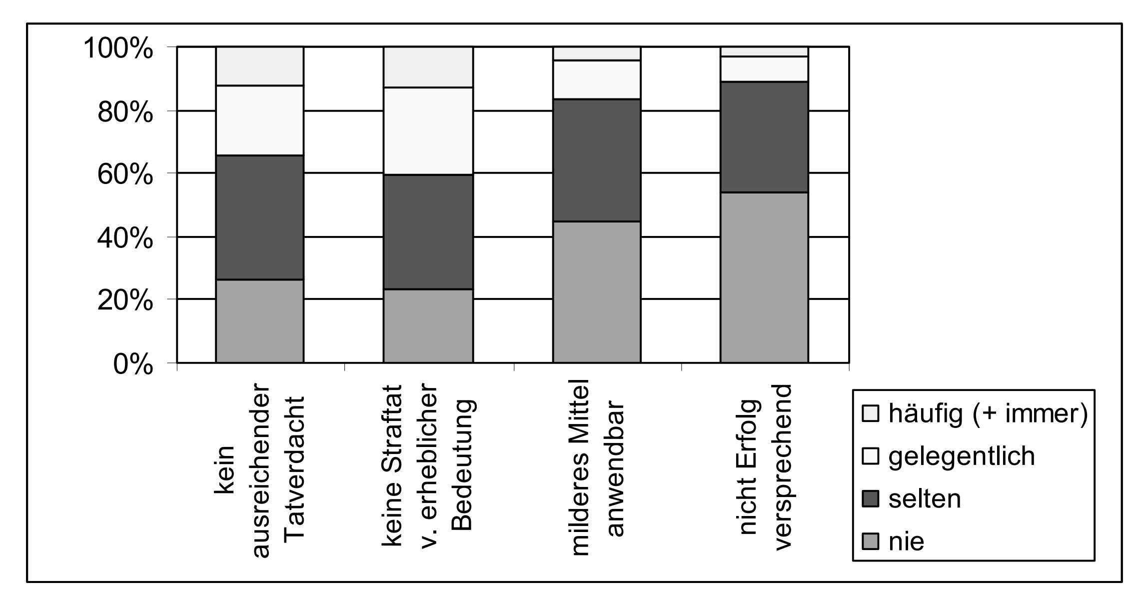


Abbildung 40



Begründungen für die Ablehnung von Anträgen



2. Aktenanalyse

Die ausgewerteten Verfahren wurden daraufhin überprüft, wer die Anordnungen in welchem Unfang erlassen hat. Auf der Grundlage des gewählten Aktenzugangs konnten Ablehnungen insoweit nicht systematisch erfasst werden (siehe oben).

a) Anteile gerichtlicher und staatsanwaltschaftlicher Anordnungen

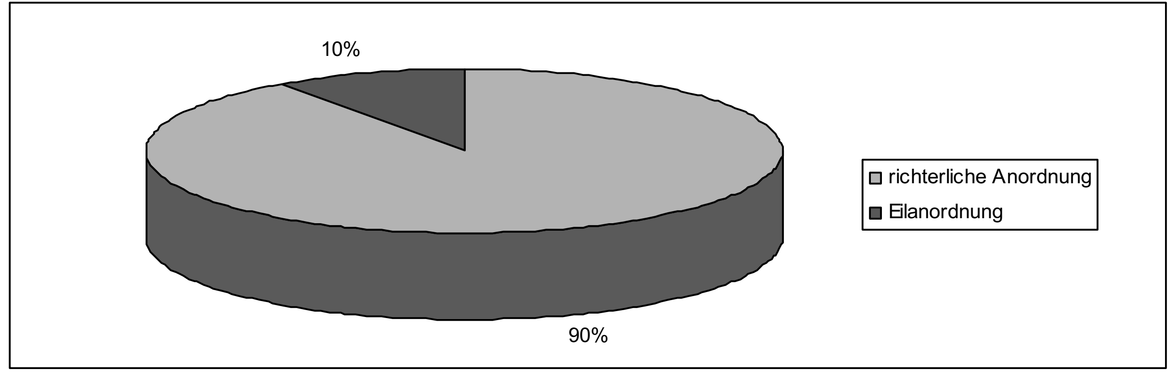
Bei 90 Prozent der Anordnungen, in denen ersichtlich war, ob eine Eilmaßnahme oder ein richterlicher Beschluss erlassen wurde, wurden die Verkehrsdatenabfragen durch den Richter angeordnet (siehe Abbildung 41). Bei 111 Anordnungen (10 Prozent) handelte es sich um Eilanordnungen. Bei ca. 10 Prozent der Anordnungen war nicht ersichtlich, ob es sich um Eilmaßnahmen oder richterliche Anordnungen handelte. Dies betrifft Fälle, bei denen kein Beschluss bzw. kein Antrag der Staatsanwaltschaft in der Akte enthalten war, aber aus anderen Umständen (z. B. Antworten der Netzbetreiber, Vermerke) ersichtlichtlich war, dass die Maßnahme angeordnet wurde[435].

[435] Einzelrecherchen konnten aus Zeitgründen nur in Einzelfällen durchgeführt werden.

Abbildung 41



Anteil richterlicher und staatsanwaltschaftlicher Anordnungen



b) Richterliche Bestätigung von Eilanordnungen

Wie Abbildung 42 zeigt, wurden die Eilanordnungen zu 69 Prozent ausdrücklich bestätigt. In 31 Prozent der Eilanordnungen (34 Fälle) fand keine aus den Akten ersichtliche Bestätigung der Eilanordnungen statt. Bei zehn dieser Eilanordnungen konnte den Akten explizit entnommen werden, dass die Maßnahmen ohne richterliche Bestätigung durchgeführt wurden. Weitere zehn dieser Eilanordnungen wurden weder ausdrücklich bestätigt, noch explizit abgelehnt, aber den Akten ließ sich entnehmen, dass die Maßnahmen (trotz fehlender Bestätigung) innerhalb der gesetzlichen Drei-Tages-Frist umgesetzt wurden. In den übrigen Fällen war weder eine Bestätigung, noch die Durchführung der Maßnahmen ersichtlich. Zu berücksichtigen ist ferner, dass an mehreren Stellen ersichtlich war, dass einige Anbieter ohne explizite Bestätigung keine Daten herausgeben. In diesen Fällen wird – um Datenverlust zu vermeiden – wohl trotz inhaltlicher Bedenken eine richterliche Bestätigung erfolgt sein. Wie viele Bestätigungen alleine deswegen erfolgten, weil sich die Polizei- und Justizbehörden darüber bewusst sind, dass die Anbieter die Herausgabe der Daten sonst verweigern würden, war aber nicht festzustellen.

Der Zeitraum, in dem die Bestätigungen erfolgten, liegt zwischen einem Tag und 21 Tagen. 38 Prozent der Eilanordnungen wurden vom Richter innerhalb eines Tages bestätigt. Weitere 14 Prozent wurden innerhalb der vorgeschriebenen drei Tage bestätigt. 17 Prozent der Eilanordnungen wurden erst später bestätigt.

c) Ablehnung, Änderung und Ergänzung von Anträgen

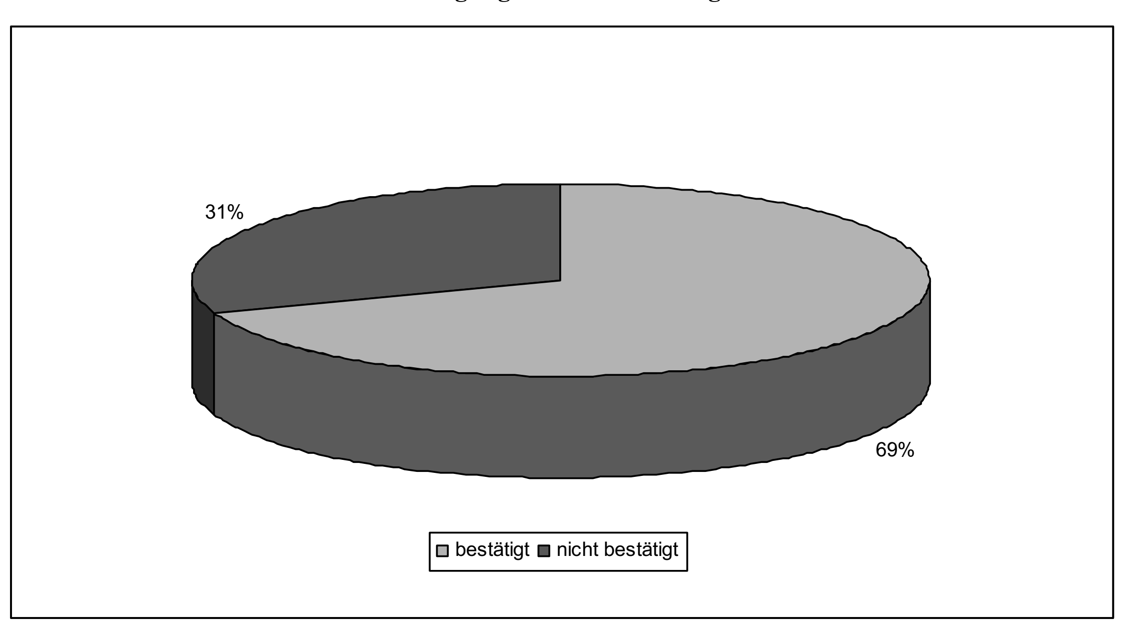
Bei 87 Prozent der Anschlüsse wurde die Verkehrsdatenabfrage wie beantragt vom Richter angeordnet. Eine ausdrückliche Ablehnung der Anträge durch den Richter erfolgte bei sechs von 1 909 Anschlüssen[436]. Diese Ablehnungen betrafen fünf Beschlüsse. Grund für die Ablehnung war das Fehlen der Voraussetzungen der §§ 100g, 100h StPO. In drei Fällen lag kein ausreichender Tatverdacht vor. Sonstige Gründe bezogen sich darauf, dass weder eine Straftat von erheblicher Bedeutung noch eine mittels Endeinrichtung begangene Straftat vorliegt sowie allgemein, dass die Voraussetzungen des § 100g I StPO nicht gegeben sind. Zudem wurden – wie bereits ausgeführt – zehn Eilanordnungen ausdrücklich nicht vom Gericht bestätigt. Bei weiteren 14 Eilanordnungen konnte den Akten keine explizite richterliche Bestätigung entnommen werden. Bei 53 Anschlüssen nahm der Richter Änderungen und Ergänzungen gegenüber dem Antrag der Staatsanwaltschaft vor. Die Änderungen betrafen vor allem die Dauer der Maßnahmen. Häufig wurde der Abfragezeitraum vom Richter erst festgelegt. Etwa zu gleichen Teilen fanden Erweiterungen und Reduzierungen der Abfragedauer durch den Richter statt. Sonstige Änderungen betrafen u.a. die korrekte Nennung der Rechtsgrundlage (z. B. statt § 12 FAG wurden §§ 100g, 100h StPO angegeben).

[436] Aufgrund des Aktenzugangs über die Netzbetreiber konnten die Ablehnungen von Anträgen nicht systematisch erfasst werden.

Abbildung 42



Bestätigung der Eilanordnungen



d) Begründungen der Anregungen, Anträge und Beschlüsse

Nach § 34 StPO ist die Anordnung der Verkehrsdatenabfrage durch den Richter zu begründen. Der normale Ablauf bei der Anordnung der Verkehrsdatenabfrage gestaltet sich – wie bereits geschildert – in der Art, dass die Polizei die Maßnahme bei der Staatsanwaltschaft anregt, die Staatsanwaltschaft einen Antrag beim Gericht stellt und das Gericht einen Beschluss erlässt. Bei Gefahr im Verzug ordnet die Staatsanwaltschaft die Maßnahmen durch eine Eilanordnung an, welche vom Richter bestätigt werden muss. Bei diesem Ablauf begründen sowohl die Polizei als auch die Staatsanwaltschaft ihre Anregung bzw. den Antrag, um die nachfolgende „Instanz“ von der Notwendigkeit der Durchführung zu überzeugen. Die Anforderungen an die Begründung des Richters sind im Einzelnen nicht konkret festgelegt. Das Bundesverfassungsgericht fordert zumindest eine richterliche Einzelfallprüfung, die sich auf die Eingriffsvoraussetzungen und die Angemessenheit des Eingriffs im konkreten Einzelfall beziehen muss.[437] Ferner soll die Anordnung auch die dem Beschuldigten zur Last gelegte Straftat sowie den Grund der Überwachung unter Angabe der Verdachts- und Beweislage, die die Maßnahme rechtfertigt, enthalten.[438]

Zur Einschätzung der Qualität der Begründungen von Polizei, Staatsanwaltschaft und vor allem des Gerichts wurden verschiedene Kriterien zugrunde gelegt, an Hand derer die Begründungen bewertet wurden. Dabei wurden im Wesentlichen die Kriterien und Kategorien verwendet, die in der Telekommunikationsüberwachungsstudie entwickelt worden sind.[439] Zu berücksichtigen ist in diesem Zusammenhang, dass die schriftlich niedergelegte Begründung nicht unbedingt etwas über den Umfang der Prüfung aussagt. Es lässt sich anhand der Akten nur überprüfen, wie z. B. der Richter die Anordnung schriftlich begründet hat. Die Intensität der inhaltlichen Auseinandersetzung lässt sich freilich über die schriftlichen Äußerungen nicht beobachten. Die Kriterien, die für die Beurteilung der Begründung herangezogen wurden, sind in Tabelle 20 dargestellt.

Die Einordnung der Begründungen erfolgte durch den jeweiligen Bearbeiter der Akte und ist insofern subjektiv

[437] BVerfG NStZ 2003, 441; *Gusy*, NStZ 2003, 403; *Meyer-Goßner*, § 100h Rn. 3.

[438] BGHSt 47, 362; *Kinzig*, StV 2004, 562.

[439] *Albrecht/Dorsch/Krüpe*, S. 220 ff.

Tabelle 20

Kategorien und Kriterien für Begründungen

Kategorien	Kriterien
Formelhaft	Keine Angabe von Gründen: – „Es wird beantragt, … (die Daten abzufragen)“ oder – „Die Voraussetzungen des § 100g StPO liegen vor“
Vordruck	Anregung/Antrag/Beschluss liegt in Form eines teilweise ausgefüllten Vordrucks vor.
Verweis auf Polizeibegründung bzw. StA-Begründung	Antrag/Beschluss verweisen auf die Polizei-/StA-Begründung
Gesetzesformel	Die Begründung enthält Passagen wie: – „Die Erforschung des Sachverhalts ist auf andere Weise aussichtslos oder wesentlich erschwert.“ – „Die Anordnung richtet sich gegen eine Person, von der auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennimmt oder weitergibt oder dass der Beschuldigte ihren Anschluss benutzt.“
Substantiell	– Auseinandersetzung mit anderen Ermittlungsmaßnahmen – Täterstrukturen werden dargelegt – umfassende Sachverhalts- und Tatverdachtsdarstellung
Verweis auf Erstbegründung	Wenn Anregung/Antrag/Beschluss auf vorherige Begründungen verweist (z. B. vorausgegangener Beschluss, aber auch Haftbefehl o.ä.)
Telefonischer Antrag/ Begründung unbekannt	Bei Hinweisen, dass Anregung/Antrag telefonisch erfolgten oder wenn die Begründung unbekannt ist

noch Tabelle 20

Kategorien	Kriterien
StA_Beschluss_Entwurf	Die Staatsanwaltschaft erstellt eine Verfügung mit dem Antrag, den beiliegenden Beschluss zu erlassen und schickt einen Beschlussentwurf mit, den der Richter nur noch unterschreiben muss. (staatsanwaltschaftliche Begründung)
Wie Antrag ausgeführt	Wenn Antrag und Beschluss (nahezu) wortgleich sind oder der Richter den mitgeschickten Beschlussentwurf der Staatsanwaltschaft lediglich unterschreibt. (richterliche Begründung)
Kurze Darstellung des SV	Wenn lediglich ein kurze Darstellung des Sachverhalts erfolgt und keine weitere Begründung abgegeben wird.
Sonstiges	Verschiedene Begründungen: Nähere Ausführungen bei den jeweiligen Begründungen von Polizei, StA und Gericht.

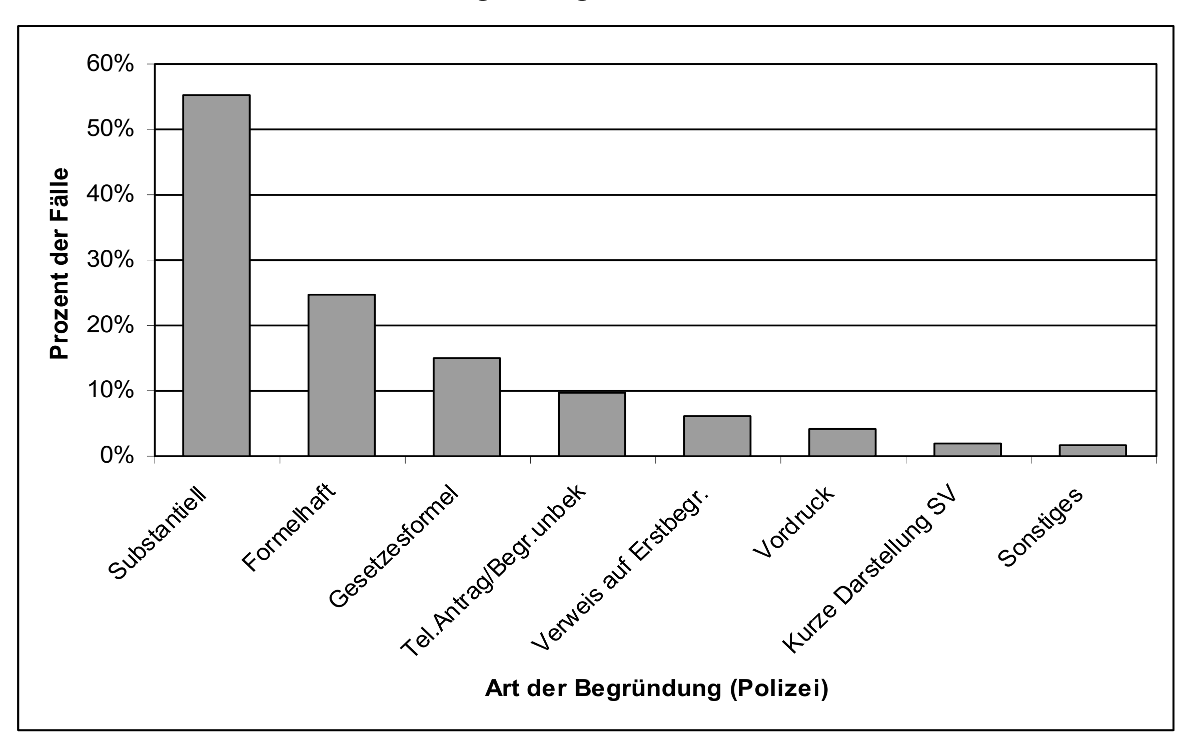
geprägt. Bei der Beurteilung der Begründungen waren Mehrfachnennungen möglich, so dass die Begründung z. B. einen Verweis auf die Begründung der Polizei enthalten kann und zudem auch den Gesetzestext wiedergeben kann (Kategorie „Gesetzesformel“).

Die Qualität der Begründung der Anregung der Maßnahmen durch die Polizei ist in Abbildung 43 dargestellt. Zu berücksichtigen ist hier, dass die Einordnung der Qualität der Begründung in eine Kategorie bei den Polizeibegründungen nicht von Beginn der Aktenauswertung an erfolgte. Erst nachdem sich herausgestellt hatte, dass auf die Begründungen der Polizei durch die Staatsanwaltschaft oftmals Bezug genommen wird und dass ein Zusammenhang zwischen der Qualität der Begründungen besteht, wurden die Polizeibegründungen wie die Begründungen der Staatsanwaltschaft und des Gerichts in Kategorien eingeordnet. Daher erfolgte eine Kategorisierung für 932 von 1 257 Beschlüssen.

Die Begründung der Polizei wurde zum größten Teil von den Bearbeitern als substantiell eingestuft (55 Prozent der

Abbildung 43

Begründungen der Polizei



Fälle). Zu 25 Prozent waren die Begründungen der Polizei nach Angabe der Bearbeiter der Akten lediglich formelhaft und zu 15 Prozent wurde der Gesetzestext mit Formulierungen wie „die Erforschung des Sachverhalts ist sonst aussichtslos oder wesentlich erschwert“ wiedergegeben. Sonstige Begründungen waren hier z. B. Verweise auf Beiakten.

Um die Einordnung etwas allgemeiner betrachten und substantielle und formelhafte Begründungen unmittelbar gegenüberstellen zu können, wurden die Begründungen „formelhaft“, „Gesetzesformel“ und „Vordruck“ zu einer Kategorie („formelhaft/kurz“) zusammengefasst und alle sonstigen Kategorien in der Kategorie „sonstige“ zusammengefasst. Diese Zuordnung der Vordruck-Fälle erfolgte vor allem aus forschungstechnischen Gründen. Denn in diesen Fällen lässt sich nicht erkennen, ob überhaupt und gegebenenfalls in welcher Intensität eine substanzielle inhaltliche Auseinandersetzung mit der Antragsbegründung tatsächlich stattgefunden hat. Eine positive Festlegung dahingehend, dass sich die Richter nicht mit dem Fall beschäftigt hätten, ist damit nicht verbunden. Ausgeschlossen werden kann dies freilich ebenso wenig. Was darüber hinaus die rechtliche Würdigung dieser Fälle anbetrifft, so ist zwar festzustellen, dass der Bundesgerichtshof – ungeachtet kritischer Stimmen in der Literatur[440] – die Verwendung von Vordrucken grundsätzlich für zulässig erachtet.[441] Allerdings muss ein Beschluss in jedem Fall erkennen lassen, dass eine Abwägung stattgefunden hat.[442] Dies ist bei der retrospektiven Aktenanalyse jedoch häufig nicht der Fall. Auch das Bundesverfassungsgericht steht dieser Praxis eher skeptisch gegenüber; es stellt explizit fest, dass ein bloßes Gegenzeichnungsverfahren den verfassungrechtlichen Anforderungen an die richterliche Überprüfungspflicht nicht entspräche.[443] Auf der Grundlage einer solchen Kategorisierung ergibt sich die in Abbildung 44 dargestellte Grundverteilung.

In der allgemeinen Betrachtung überwiegen eindeutig die substantiellen Begründungen der Polizei bei der Anregung (55 Prozent). Unterschiede entlang der Bundesländer sind aus Abbildung 45 und Abbildung 46 ersichtlich, wobei letztere wiederum die zusammengefasste Variante darstellt.

Dabei fällt auf, dass vor allem in Baden-Württemberg die substantiellen Begründungen der Anregungen der Polizei überwiegen (69 Prozent). Dagegen sind die Begründungen der Polizei in Mecklenburg-Vorpommern häufiger formelhaft (41 Prozent) als substantiell (27 Prozent). In diesem Bundesland sind auch die meisten telefonischen Anregungen zu verzeichnen. Die Wiedergabe der Gesetzesformel erfolgt am häufigsten in Berlin, wobei zu berücksichtigen ist, dass hier auch die substantiellen Begründungen eindeutig überwiegen.

Bei der allgemeinen Betrachtung (Abbildung 46) kommen diese Unterschiede in den Begründungen der Polizei in den verschiedenen Bundesländern noch deutlicher zur Geltung. In Baden-Württemberg und Nordrhein-Westfalen überwiegen eindeutig die substantiellen Begründungen, während in Mecklenburg-Vorpommern eindeutig die formelhaften Begründungen der Polizei häufiger sind. In Berlin überwiegen zwar die substantiellen Begründungen, aber auch der Anteil an formelhaften Begründungen ist relativ groß.

[440] *Kinzig*, StV 2004, S. 566; *Weßlau*, StV 1996, S. 579.
[441] BGH mit Anmerkung *Weßlau*, StV 1996, S. 579; BGH mit Anmerkung *Bernsmann*, NStZ 1997, S. 250.
[442] Vgl. dazu auch *Albrecht/Dorsch/Krüpe*, 2003, S. 217.
[443] BVerfG, NJW 2003, S. 1787, 1982 = NStZ 2003, S. 441, 443.

Abbildung 44

Begründungen der Polizei (allgemeine Betrachtung)

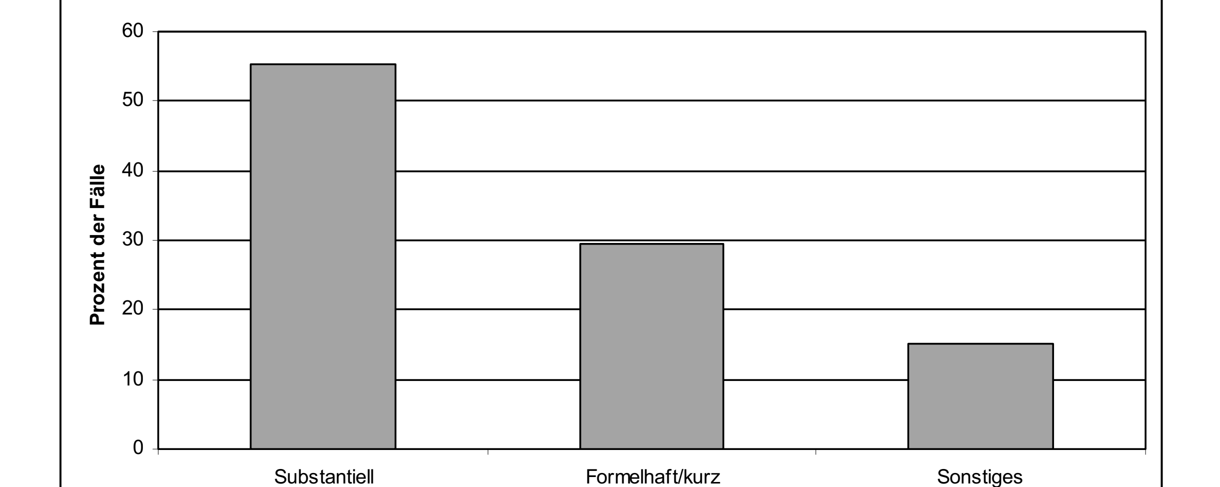


Abbildung 45



Begründungen der Polizei nach Bundesländern

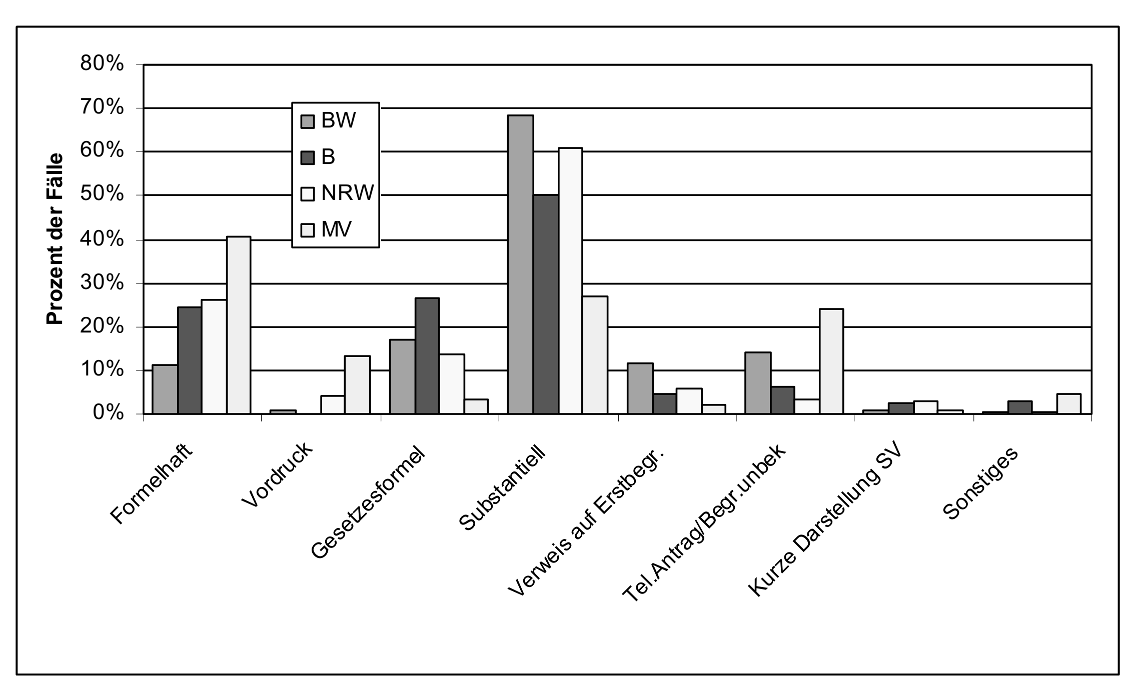
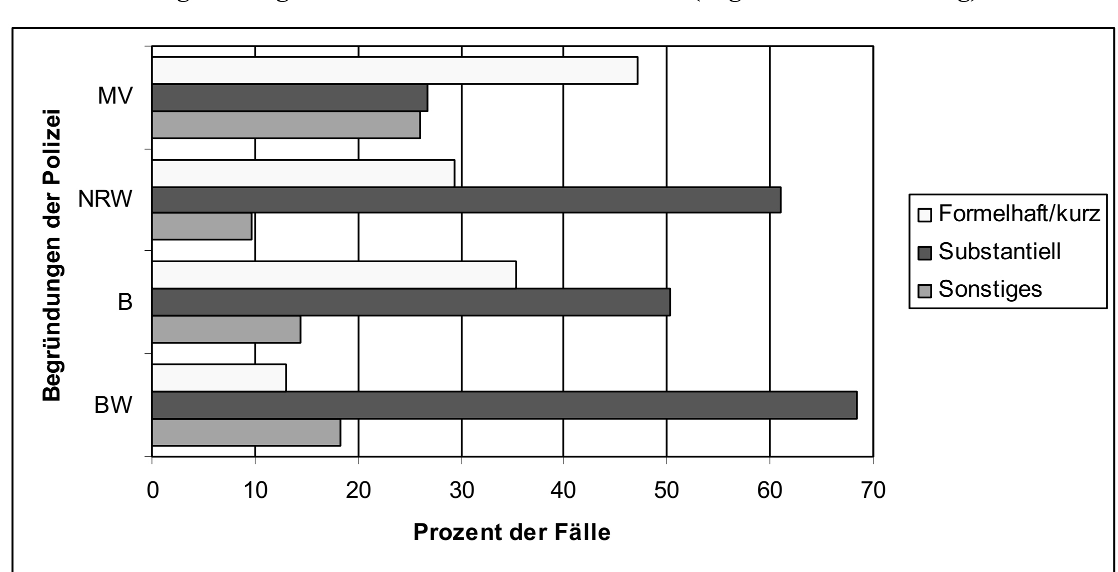


Abbildung 46

Begründungen der Polizei nach Bundesländern (allgemeine Betrachtung)



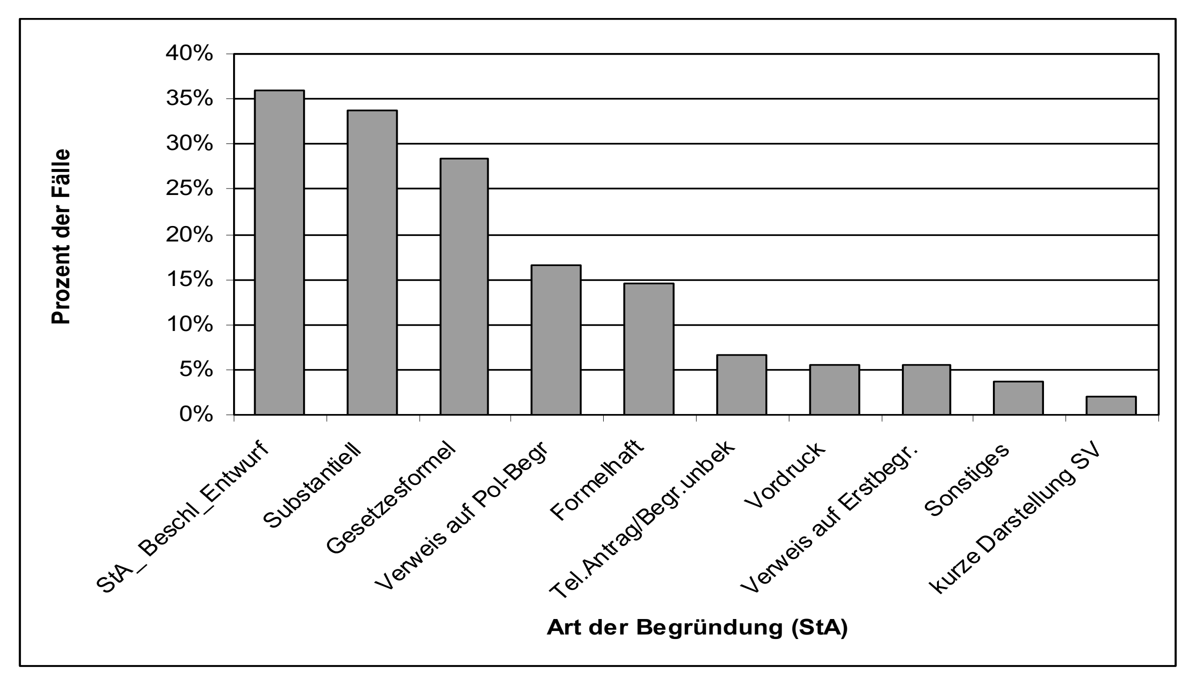
Aus Abbildung 47 lässt sich die Qualität der Begründungen der Anträge auf Durchführung einer Maßnahme nach §§ 100g, 100h StPO durch die Staatsanwaltschaft entnehmen. Bei 55 Beschlüssen war kein Antrag der Staatsanwaltschaft in den Akten enthalten. Auch hier sind wiederum Mehrfachnennungen möglich gewesen. Eilanordnungen wurden hierbei nicht berücksichtigt. Diese werden im Folgenden noch separat betrachtet. Am häufigsten ist bei der Beantragung die Übersendung eines Beschlussentwurfes an das Gericht durch die Staatsanwaltschaft, den der Ermittlungsrichter nur noch zu unterschreiben braucht (36 Prozent). Ebenfalls sehr häufig – und dies ist oftmals mit der ersten Kategorie einhergegangen – ist die substantielle Begründung der Anträge (34 Prozent). Nur geringfügig seltener wurde von den Staatsanwälten nur der Gesetzestext wiedergegeben (28 Prozent) und auch der Verweis auf die Polizeibegründung (17 Prozent) sowie eine formelhafte Begründung (15 Prozent) waren noch relativ häufig. Sonstige Begründung war hier z. B. dass es sich lediglich um einen Änderungsantrag ohne weitere Begründung handelte.

Bei der allgemeinen Betrachtung, welche in Abbildung 48 dargestellt ist, überwiegen dementsprechend die sonstigen Begründungen der Staatsanwaltschaft, da von dieser Kategorie die Übersendung eines Beschlussentwurfes sowie der Verweis auf die Polizeibegründung erfasst sind und diese einen großen Teil der Begründungen darstellen. Ansonsten überwiegt aber die substantielle Begründung (34 Prozent) gegenüber der formelhaften Begründung (17 Prozent) des Antrags durch die Staatsanwälte.

Auch bei der Begründung des Antrags auf Durchführung einer Maßnahme nach §§ 100g, 100h StPO zeigten sich Unterschiede entlang der Bundesländer (siehe Abbildung 49). Auffällig ist vor allem, dass die Übersendung eines vorgefertigten Beschlussentwurfes von der Staatsanwaltschaft an den Richter in Baden-Württemberg mit einem Anteil von 86 Prozent der Fälle fast schon den Regelfall darstellt. In den übrigen Bundesländern dagegen war dies nicht die so deutlich häufigste Kategorie. In Berlin war die Zitierung der Gesetzesformel am häufigsten (48 Prozent). In Nordrhein-Westfalen überwog die substantielle Begründung des Antrags durch die Staatsanwaltschaft (43 Prozent). In Mecklenburg-Vorpommern herrschten formelhafte Begründungen der Anträge vor (31 Prozent) und der Anteil an vorformulierten Beschlussentwürfen war hier ebenfalls recht hoch (27 Prozent).

Abbildung 47

Begründung der Staatsanwaltschaft



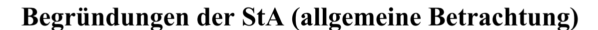


Abbildung 48

Begründungen der StA (allgemeine Betrachtung)

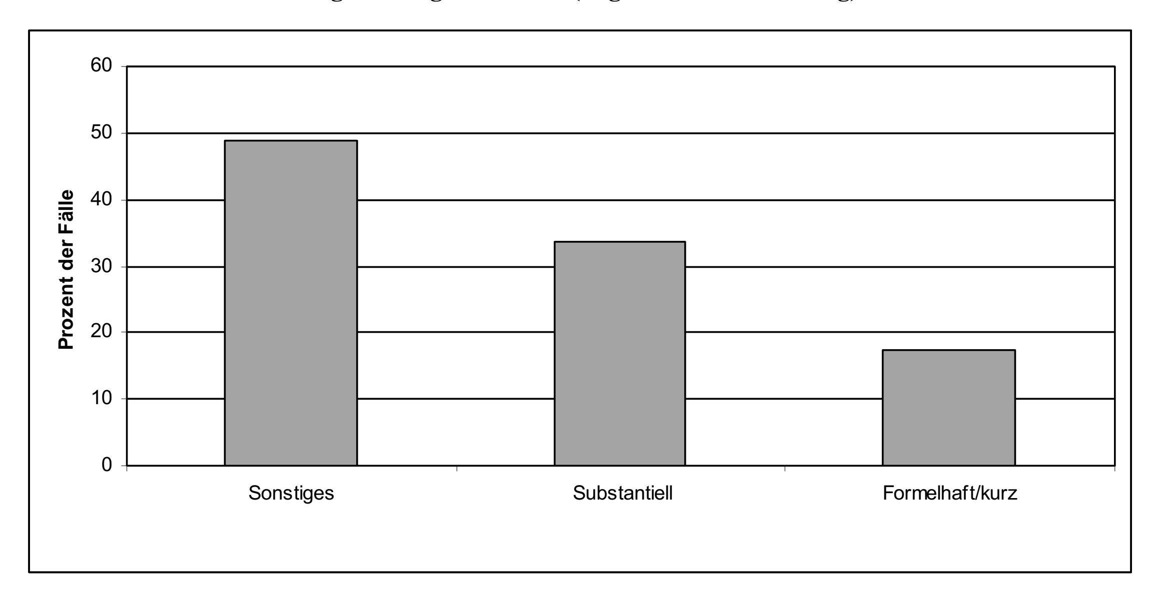
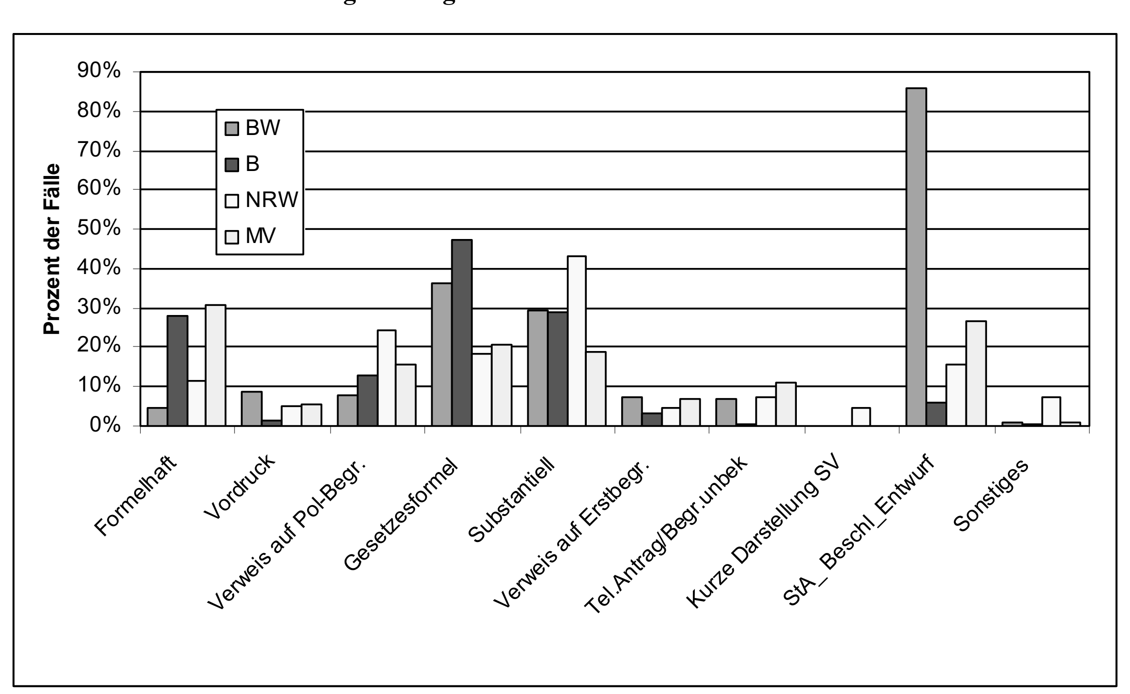


Abbildung 49

Begründungen der StA nach Bundesländern



Die allgemeine Betrachtung verdeutlicht diese Unterschiede der Begründungen der Anträge durch die Staatsanwälte noch einmal (siehe Abbildung 50). In Baden-Württemberg und Mecklenburg-Vorpommern überwiegen durch die Zusendung der Beschlussentwürfe die sonstigen Begründungen. In Baden-Württemberg überwiegen aber ansonsten die substantiellen Begründungen, während in Mecklenburg-Vorpommern die formelhaften Begründungen häufiger waren. In Nordrhein-Westfalen sind sonstige und substantielle Begründungen am häufigsten. In Berlin überwiegen durch die häufige Verwendung der Gesetzesformel und durch häufige formelhafte Begründungen die formelhaften, kurzen Begründungen.

Bei den Begründungen der Beschlüsse durch die Ermittlungsrichter nach §§ 100g, 100h StPO überwiegen – wie Abbildung 51 zeigt – diejenigen, die wie der Antrag der Staatsanwaltschaft ausgeführt sind[444]. Am häufigsten wurde demnach der Beschlussentwurf, den die Staatsanwaltschaft an das Gericht sandte, unterschrieben oder der Antrag der Staatsanwaltschaft fast wortgleich übernommen (49 Prozent). Zu berücksichtigen ist hier, dass bei bloßer Unterschrift des substantiell ausgeführten Beschlussentwurfs der Staatsanwaltschaft die Begründung des Richters nicht ebenfalls als substantiell eingestuft wurde, da es sich um die bloße Übernahme der Begründung handelte. Dabei wird insbesondere auch die schon erwähnte Rechtsprechung des Bundesverfassungsgerichts zugrunde gelegt, wonach sich die richterliche Überprüfung eben nicht in einem reinen Gegenzeichungsverfahren erschöpfen dürfe.[445]

[444] Hier sind wiederum Mehrfachnennungen möglich.
[445] Siehe dazu oben Fn. 443.

Zu 25 Prozent wurden eigene substantielle Begründungen für den Beschlusserlass abgegeben und zu 24 Prozent wurde der Gesetzeswortlaut (z. B. „es ist davon auszugehen, dass der Anschlussinhaber Mitteilungen für den Beschuldigten entgegennimmt“ oder „die Erforschung des Sachverhalts ist ohne die Abfrage der Daten aussichtslos oder wesentlich erschwert“) zitiert. Ein Verweis auf die Polizeibegründung spielt fast keine Rolle. Unter „sonstiges“ wurden u. a. Begründungen eingeordnet, wenn es sich lediglich um einen Änderungsbeschluss handelte oder ein Beschluss nicht beilag, aber an anderen Stellen in der Akte ersichtlich war, dass es einen Beschluss gegeben haben muss. Darüber hinaus gab es 29 Fälle, in denen kein Beschluss in der Akte war.

In der allgemeinen Betrachtung (siehe Abbildung 52) überwiegen – aufgrund des häufigen Vorkommens der mit dem Antrag wortgleich übereinstimmenden Begründungen – die sonstigen Begründungen. Ansonsten halten sich die substantiellen und die formelhaften Begründungen nahezu die Waage, wobei die substantiellen Begründungen etwas häufiger sind.

Die Qualität der Begründungen der Beschlüsse unterscheidet sich in den vier zu untersuchenden Bundesländern (Abbildung 53). Entsprechend der häufigen Vorformulierung der Beschlüsse durch die Staatsanwaltschaft überwiegen bei den richterlichen Begründungen in Baden-Württemberg erwartungsgemäß diejenigen, die dem Antrag der Staatsanwaltschaft vom Wortlaut her entsprechen, bei weitem. Auch in den anderen Bundesländern kommen diese Beschlüsse häufig vor. In Berlin wird etwas häufiger der Gesetzeswortlaut wiederholt, was ebenfalls dem Bild der Begründungen der Staatsanwaltschaft entspricht.

Abbildung 50



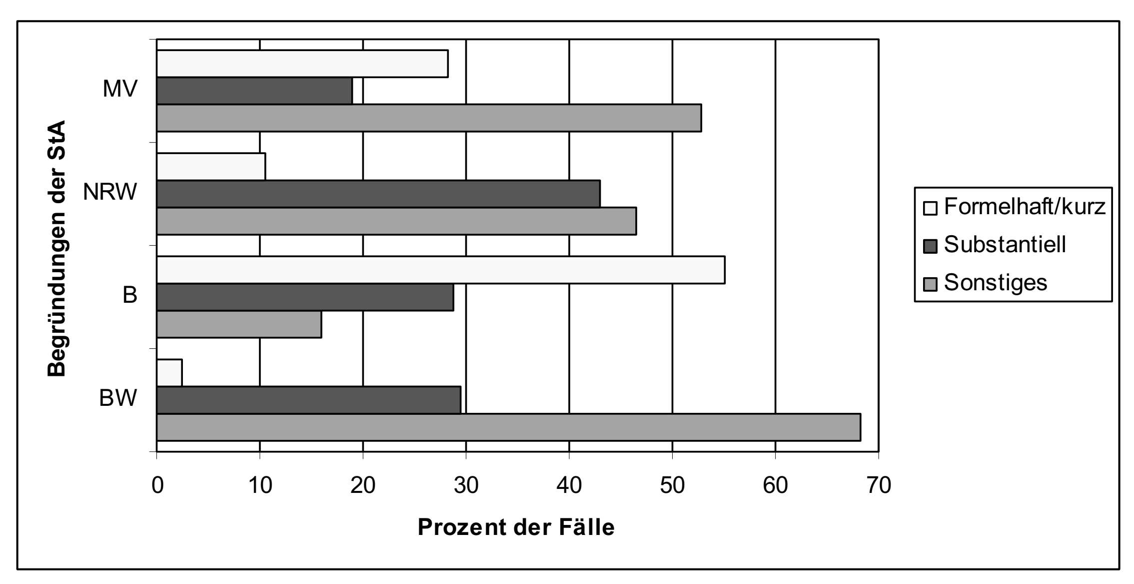


Abbildung 51



Begründungen der Richter

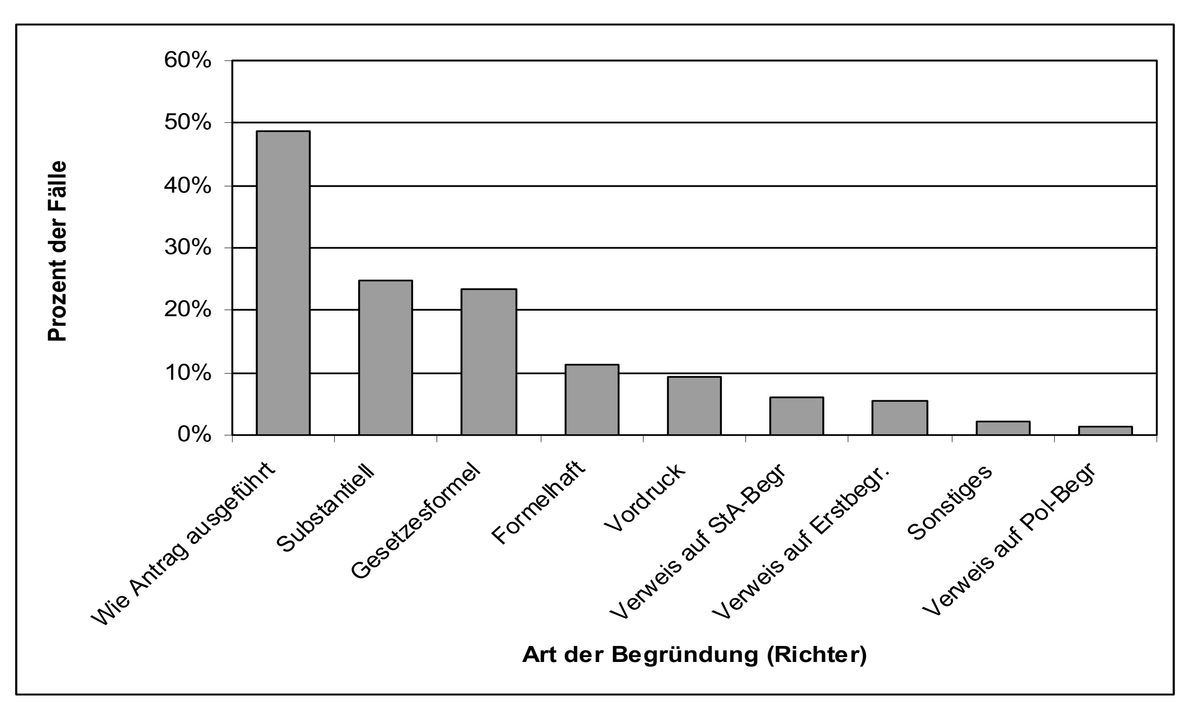


Abbildung 52

Begründungen der Richter (allgemeine Betrachtung)

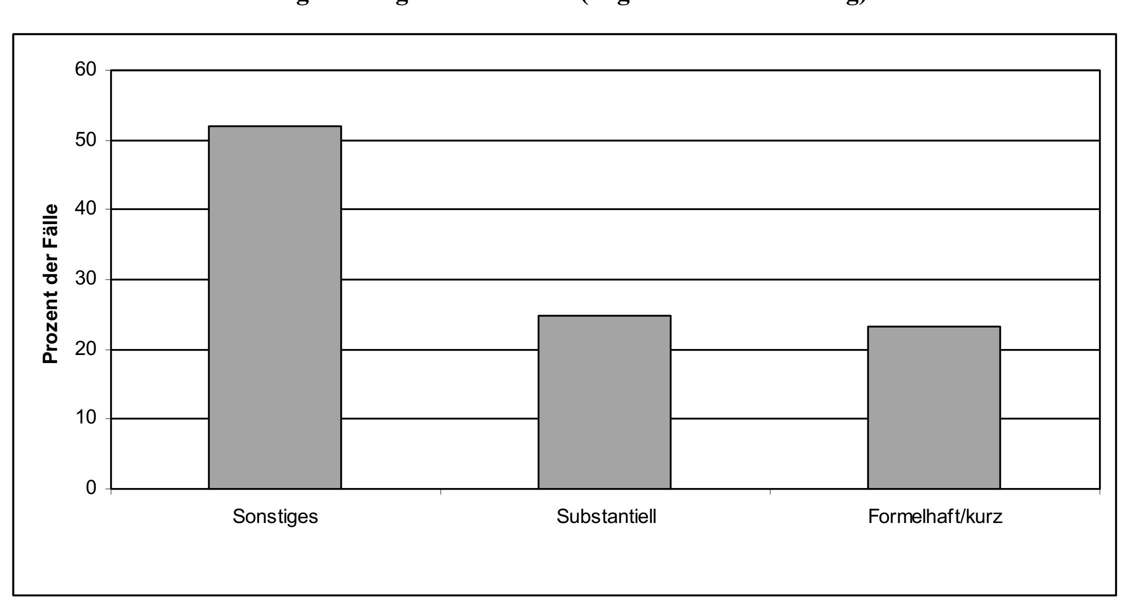
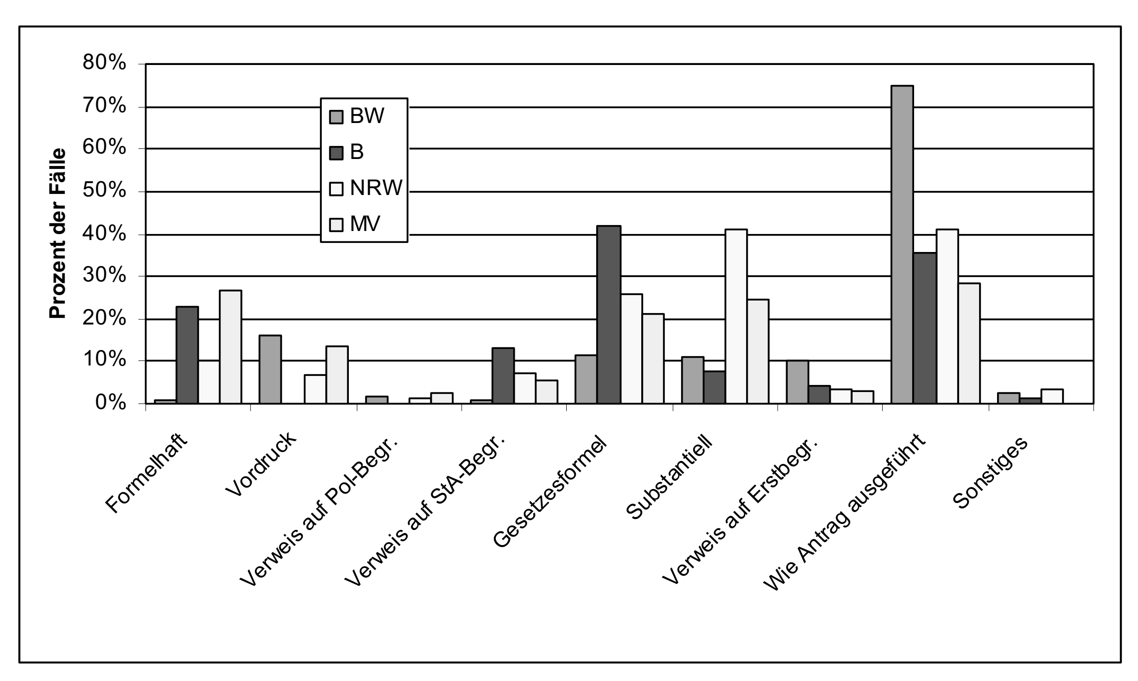


Abbildung 53

Begründungen der Richter nach Bundesländern



Ebenso häufig wie Beschlüsse, die dem Antrag der Staatsanwaltschaft entsprechen, sind in Nordrhein-Westfalen substantiell begründete Beschlüsse. In Mecklenburg-Vorpommern kommen formelhafte Begründungen der Beschlüsse etwas häufiger vor als substantielle Ausführungen, wobei auch relativ häufig lediglich der Gesetzeswortlaut zitiert wird.

Zusammengefasst stellen sich die Begründungen der Beschlüsse durch die Ermittlungsrichter unterschieden nach Bundesländern wie in Abbildung 54 gezeigt dar. In Baden-Württemberg überwiegen aufgrund der häufigen, den Anträgen der Staatsanwaltschaft entsprechenden Beschlüsse die sonstigen Begründungen. Ansonsten sind die Begründungen etwa zu gleichen Teilen substantiell und formelhaft begründet. In Berlin überwiegen neben den sonstigen Begründungen der Beschlüsse eindeutig die formelhaften Begründungen der Beschlüsse durch die Ermittlungsrichter. Dies beruht vor allem auf der häufigen Verwendung der Gesetzesformeln.

In Nordrhein-Westfalen sind eindeutig substantielle Begründungen häufiger als formelhafte. Der große Anteil an sonstigen Begründungen beruht auf der Vielzahl der den Anträgen entsprechenden Beschlüsse. In Mecklenburg-Vorpommern sind die Begründungen häufiger formelhaft als substantiell.

Unterschiede bei den Begründungen von Staatsanwaltschaft und Gericht zeigten sich dann, wenn substantielle Begründungen vorausgegangen waren. Wenn die Begründung der Polizei substantiell war, war auch die Begründung der Staatsanwaltschaft häufig substantiell. Ebenso verhielt es sich zwischen den Begründungen der Staatsanwaltschaft und des Gerichts. Die Begründungen des Gerichts waren häufiger substantiell, wenn zuvor die Begründungen der Staatsanwaltschaft substantiell waren. Diese Abhängigkeit der Qualität der Begründung von der vorausgehenden war jedoch nicht zwischen der Begründung der Polizei und des Gerichts zu bemerken. Zwischen einer substantiellen Begründung der Polizei und einer substantiellen Begründung des Gerichts bestand kein so starker Zusammenhang wie bei den beiden anderen Konstellationen.

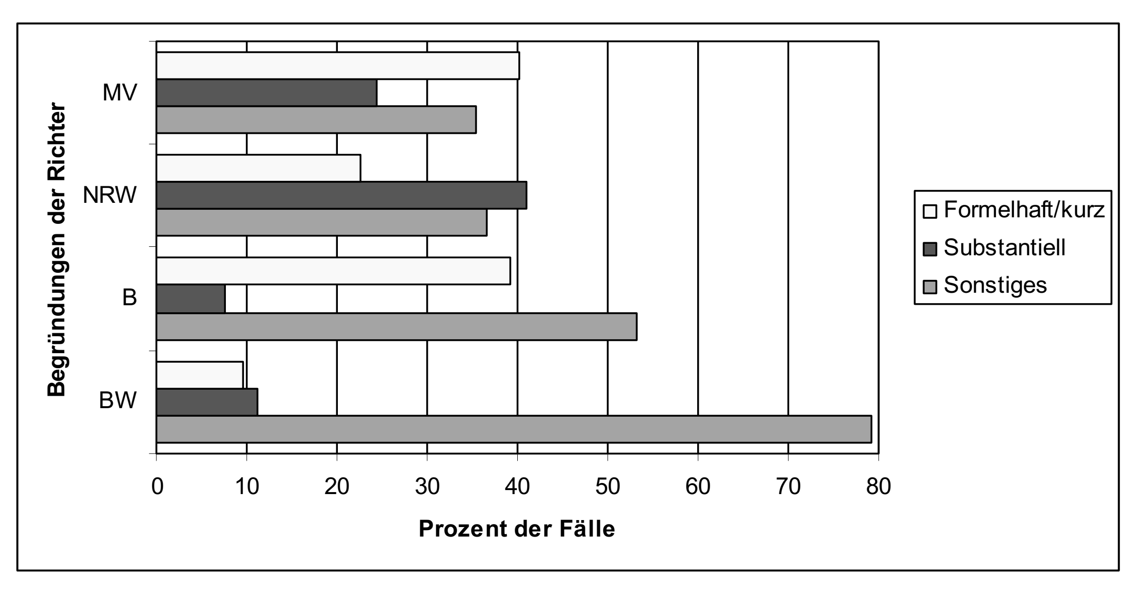
Diese Unterschiede, wenn substantielle Begründungen vorausgegangen waren, waren entlang der Bundesländer nicht immer signifikant. In Baden-Württemberg konnten keine wesentlichen Unterschiede festgestellt werden, wenn eine substantielle Begründung vorausging. Wohl aber sind in Berlin und Nordrhein-Westfalen ähnliche signifikante Zusammenhänge wie im Gesamten festzustellen. In Mecklenburg-Vorpommern bestand kein Zusammenhang zwischen der Begründung der Polizei und der Begründung der Staatsanwaltschaft, wohl aber zwischen der Begründung der Staatsanwaltschaft und der des Gerichts und in leicht abgeschwächter Form auch zwischen der Begründung der Polizei und der des Gerichts.

In etwa einem Viertel der Fälle, in denen die Staatsanwaltschaft einen Beschlussentwurf an das Gericht schickte, wurde dieser Entwurf von den Bearbeitern als substantiell bewertet. Jedoch wurde in keinem Fall der von dem Gericht bloß unterschriebene Beschlussentwurf als substantiell angesehen, da der Richter in diesem Fall

Abbildung 54



Begründungen des Gerichts nach Bundesländern (allgemeine Betrachtung)



keine eigene Begründung abgegeben hat. Ob – und gegebenenfalls in welcher Intensität – eine richterliche Auseinandersetzung mit dem Fall tatsächlich stattgefunden hat, lässt sich diesen Beschlüssen jedenfalls nicht entnehmen. Anträge der Staatsanwaltschaft, die den Gesetzestext wiedergaben, enthielten nach der Einschätzung der Bearbeiter in etwa einem Viertel der Fälle auch eine substantielle Begründung. Wenn ein Vordruck von der Staatsanwaltschaft verwendet wurde, wurde der Antrag fast nie als substantiell bewertet.

e) Begründungen der Eilanordnungen und richterlichen Bestätigungen

Die Qualität der Begründungen der Staatsanwaltschaft bei von ihr erlassenen Eilanordnungen, ergibt sich aus Abbildung 55. Hier wurden dieselben Kategorien und Kriterien zugrunde gelegt wie bei den Begründungen der Anträge durch die Staatsanwaltschaft.

Dabei fällt auf, dass bei Erlass einer Eilanordnung am häufigsten Vordrucke verwendet wurden, formelhafte Begründungen abgegeben wurden und der Gesetzeswortlaut zitiert wurde. Relativ häufig ist jedoch immer noch die substantielle Begründung.

Die zusammengefasste Form der Begründungen macht noch einmal das eindeutige Überwiegen der formelhaften Begründungen deutlich (siehe Abbildung 56).

Die formelhaften Begründungen (55 Prozent) sind mehr als doppelt so häufig wie die substantiell begründeten Eilanordnungen (25 Prozent).

In den Bundesländern sind Unterschiede bei der Qualität der Begründung der Eilanordnungen durch die Staatsanwaltschaft festzustellen (Abbildung 57). Aufgrund der relativ geringen Anzahl an Eilanordnungen (111), beschränken sich die Ausführungen auf eine allgemeine Betrachtung der Begründungen.

Mecklenburg-Vorpommern fällt mit einem weit überwiegenden Vorkommen von formelhaft begründeten Eilanordnungen auf. Dies beruht – neben sehr häufigen eindeutig als formelhaft einzustufenden Begründungen – auch auf der häufigen Verwendung von Vordrucken, welche von der Gestaltung her gar nicht auf eine substantielle Begründung hin angelegt sind. Auch in Berlin überwiegen die formelhaft begründeten Eilanordnungen die substantiell begründeten bei Weitem. Dies ist wiederum auf das häufige Zitieren des Gesetzeswortlauts zurückzuführen. Das ist auch einer der Gründe für häufige formelhafte Begründungen in Nordrhein-Westfalen, wobei dort hinzukommt, dass häufig Vordrucke verwendet wurden. In Baden-Württemberg überwiegen dagegen die substantiell begründeten Eilanordnungen. Auch die sonstigen Begründungen sind sehr häufig, was wiederum auf das Zusenden von Beschlussentwürfen durch die Staatsanwaltschaft zurückzuführen ist.

Die Qualität der Begründungen bei den richterlichen Bestätigungen der Eilanordnungen ist in Abbildung 58 dargestellt. Am häufigsten sind sonstige Begründungen (27 Prozent, 24 Nennungen). Hierzu zählen Fälle, in denen die Eilanordnungen nur richterlich bestätigt wurden ohne jegliche Begründung (elf Nennungen). Des Weiteren fallen unter diese Kategorie die Ablehnungen der richterlichen Bestätigung sowie die Fälle, in denen aus der Akte nicht ersichtlich ist, ob die Eilanordnung bestätigt wurde. Ähnlich häufig sind daneben formelhafte Begründungen durch den Richter und die Wiedergabe des Gesetzestextes.

Abbildung 55

Begründungen der StA bei Eilanordnungen

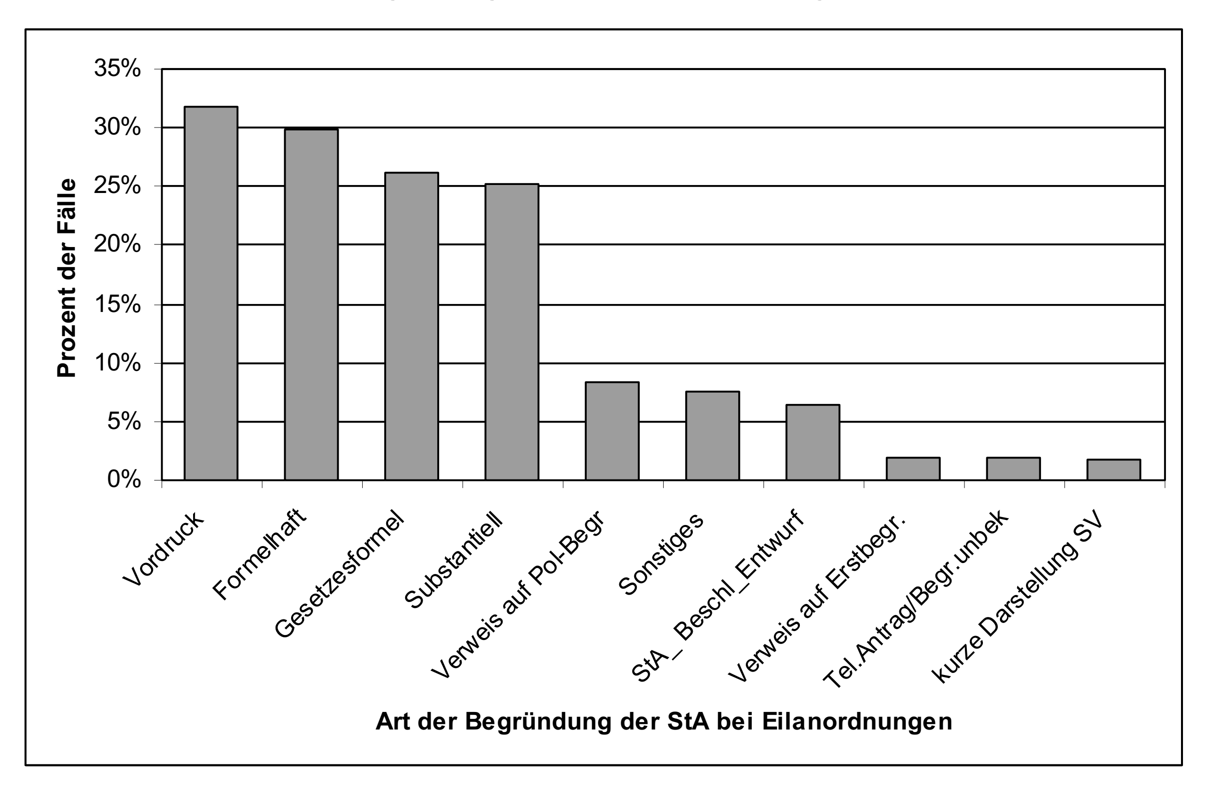


Abbildung 56

Begründungen der StA bei Eilanordnungen (allgemeine Betrachtung)

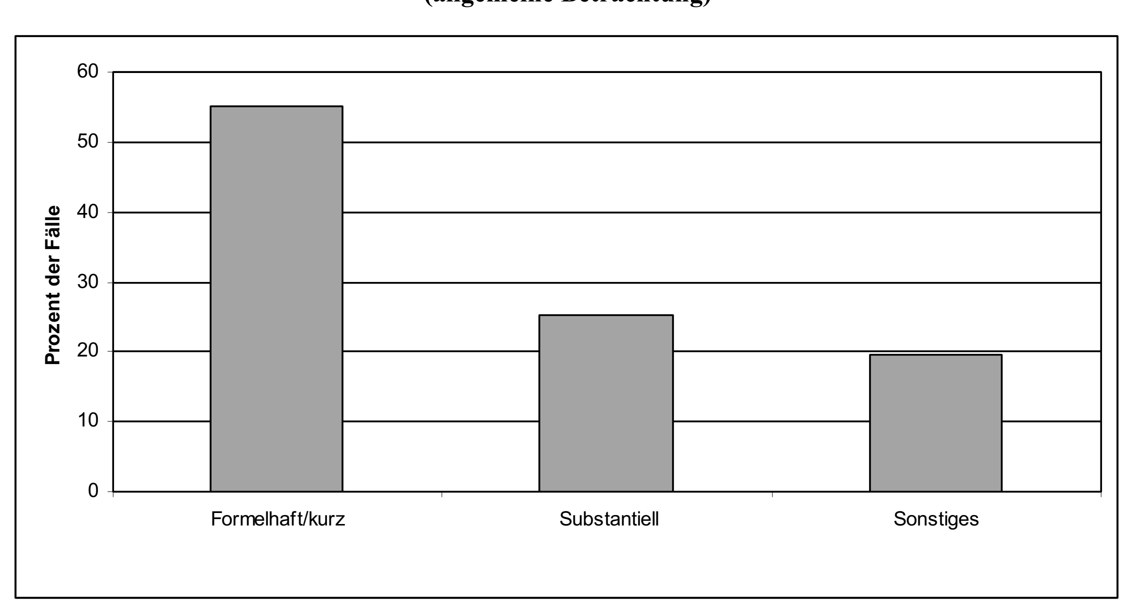


Abbildung 57



Begründungen der Eilanordnungen durch die StA nach Bundesländern (allgemeine Betrachtung)

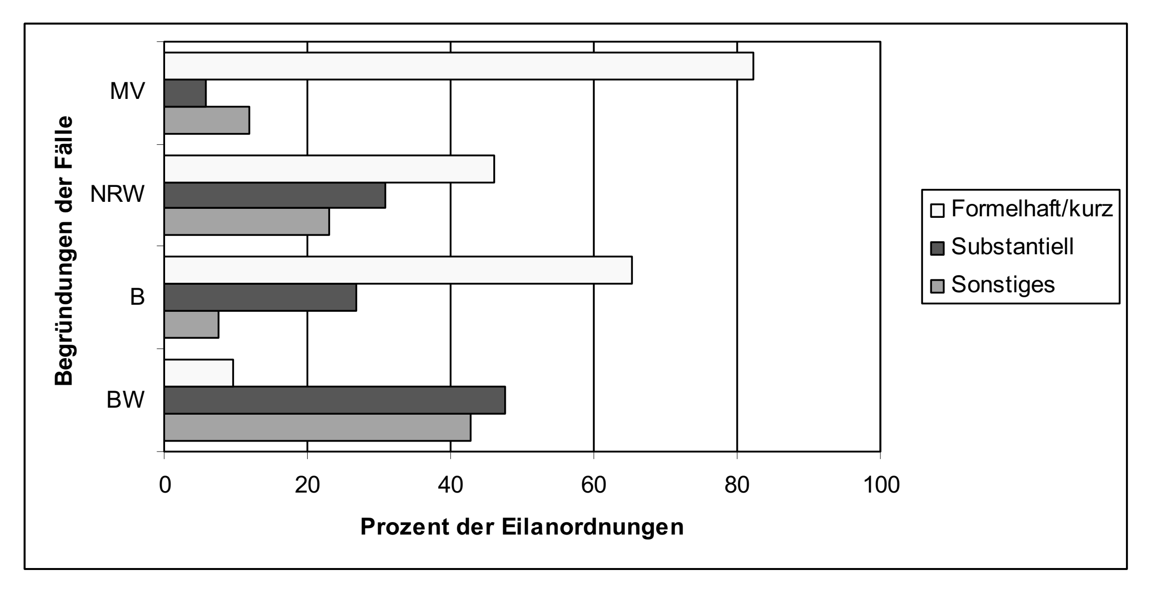
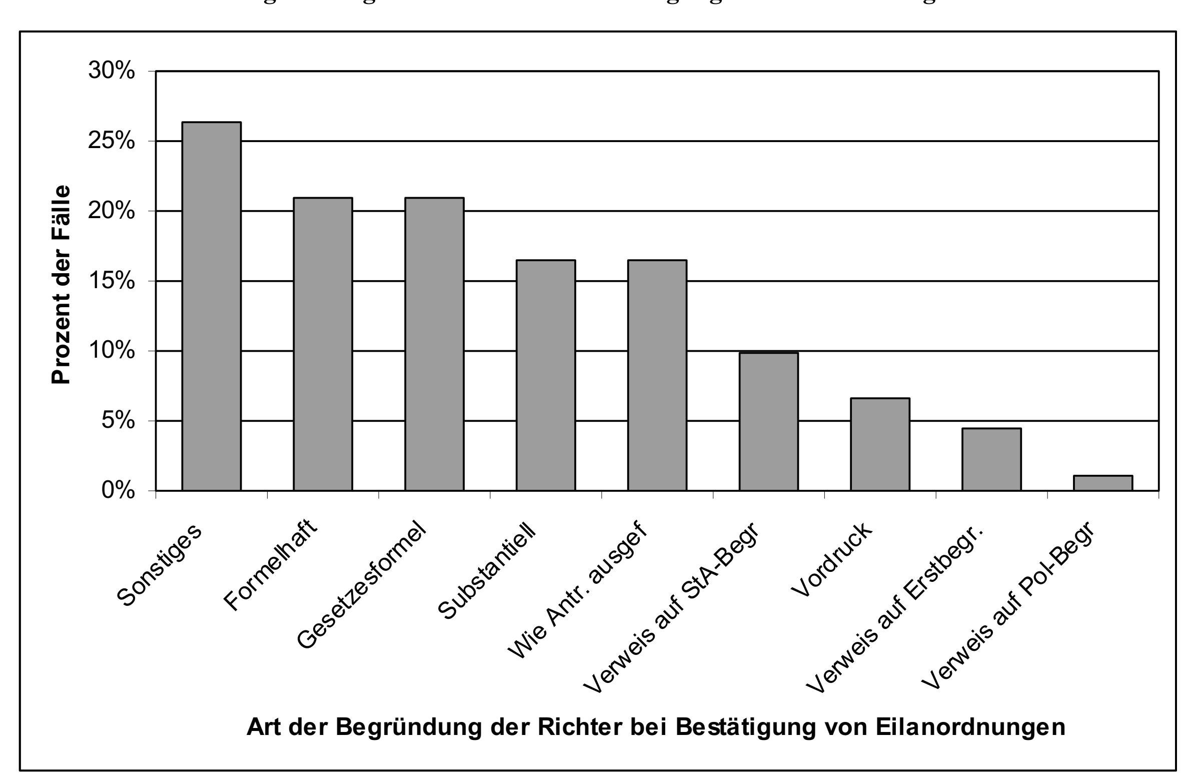


Abbildung 58

Begründungen der Richter bei Bestätigung von Eilanordnungen



Die allgemeine Darstellung der Begründungen von richterlichen Bestätigungen der Eilanordnungen zeigt noch einmal das eindeutige Überwiegen der formelhaften gegenüber den substantiellen Begründungen (Abbildung 59).

Auch hinsichtlich der Begründungen der richterlichen Bestätigungen der Eilanordnungen gibt es Unterschiede entlang der Bundesländer (siehe Abbildung 60).

In Berlin gab es keinen einzigen substantiell begründeten Bestätigungsbeschluss. In allen Bundesländern sind die sonstigen Begründungen (z. B. wie im Antrag ausgeführt, reine Bestätigung ohne Begründung usw.) sehr häufig.

Abbildung 59

Begründungen der Richter bei Bestätigung von Eilanordnungen (allgemeine Betrachtung)

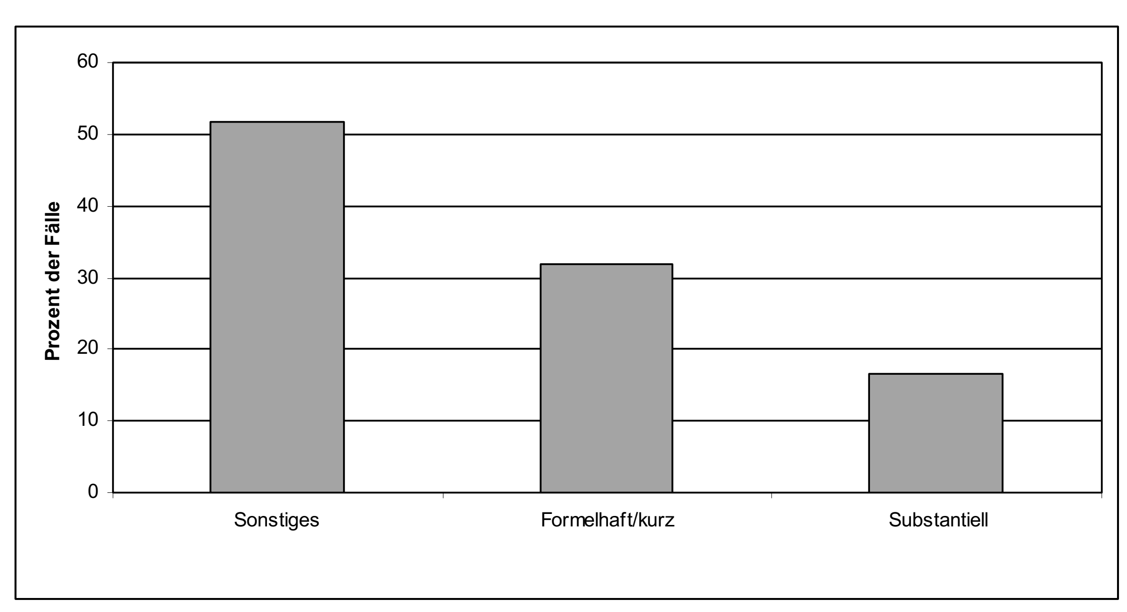
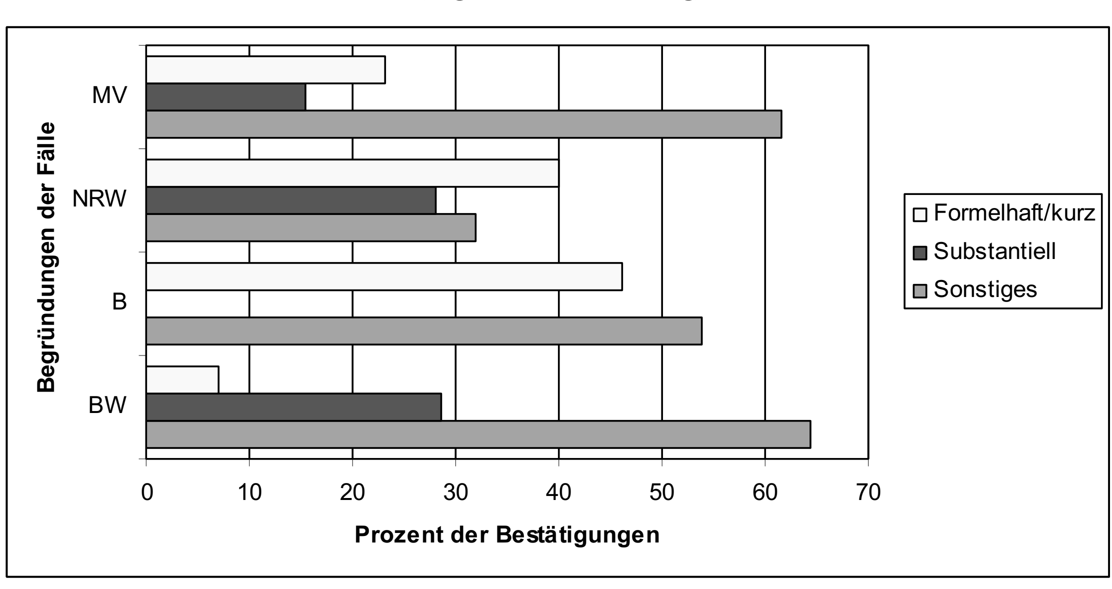


Abbildung 60

Begründungen der richterlichen Bestätigungen nach Bundesländern (allgemeine Betrachtung)



Abgesehen von Baden-Württemberg überwiegen daneben bei allen Bundesländern die formelhaften Begründungen.

f) Begründungen der Verlängerungen

In 53 Fällen wurden die Maßnahmen verlängert. Bei 48 der Verlängerungsbeschlüsse konnte den Akten explizit eine Begründung des Richters entnommen werden. Welcher Qualität die Begründungen der Verlängerungen waren, lässt sich Abbildung 61 entnehmen. In Bezug auf die Qualität der Begründungen wurde hier auf die gleichen Kategorien und Kriterien abgestellt wie bei der Begründung der Ausgangsbeschlüsse. Auch hier konnten einer Begründung mehrere Kategorien zugeordnet werden. Mehrfachnennungen waren möglich.

44 Prozent der Verlängerungsbeschlüsse waren formelhaft begründet. Es wurde also lediglich angeordnet, dass der ursprüngliche Beschluss verlängert werden soll. Bei 30 Prozent dieser Beschlüsse erfolgte eine substantielle Begründung, warum eine Verlängerung angeordnet wird. Ein Verweis auf die Erstbegründung fand in 21 Prozent der Verlängerungsbeschlüsse statt. Zu je 13 Prozent wurde ein Vordruck verwendet und auf die Polizeibegründung verwiesen. Sonstige Begründungen wie eine ganz kurze Begründung oder die Verwendung des gleichen Wortlauts wie beim ursprünglichen Beschluss, erfolgten ebenfalls in 13 Prozent dieser Beschlüsse. Gesetzesformeln wie „die Ermittlungen sind sonst aussichtslos oder wesentlich erschwert“ wurden in 8 Prozent der Verlängerungsbeschlüsse verwendet.

g) Begründungen differenziert nach Delikten

Die Qualität der Begründungen von Polizei, Staatsanwaltschaft und Gericht variiert je nach zugrundeliegendem Delikt.

Bei zugrundeliegenden Katalogdelikten (Abbildung 62) wurden von den Bearbeitern der Akten insgesamt substantiellere Ausführungen der Polizei festgestellt als bei Delikten, die nicht unter den Katalog des § 100a Satz 1 StPO fallen. Am substantiellsten begründet waren innerhalb der Katalogdelikte Anregungen der Verkehrsdatenabfrage wegen gewerbsmäßiger Hehlerei bzw. Bandenhehlerei, wegen Verstößen gegen das Ausländerrecht, wegen Geld- und Wertpapierfälschungen, schweren Bandendiebstählen und Betäubungsmitteldelikten. Formelhafte Begründungen bei zugrundeliegenden Katalogdelikten waren bei Straftaten gegen die persönliche Freiheit und Geldwäsche zu verzeichnen.

Abbildung 61

Begründung der Verlängerungsbeschlüsse

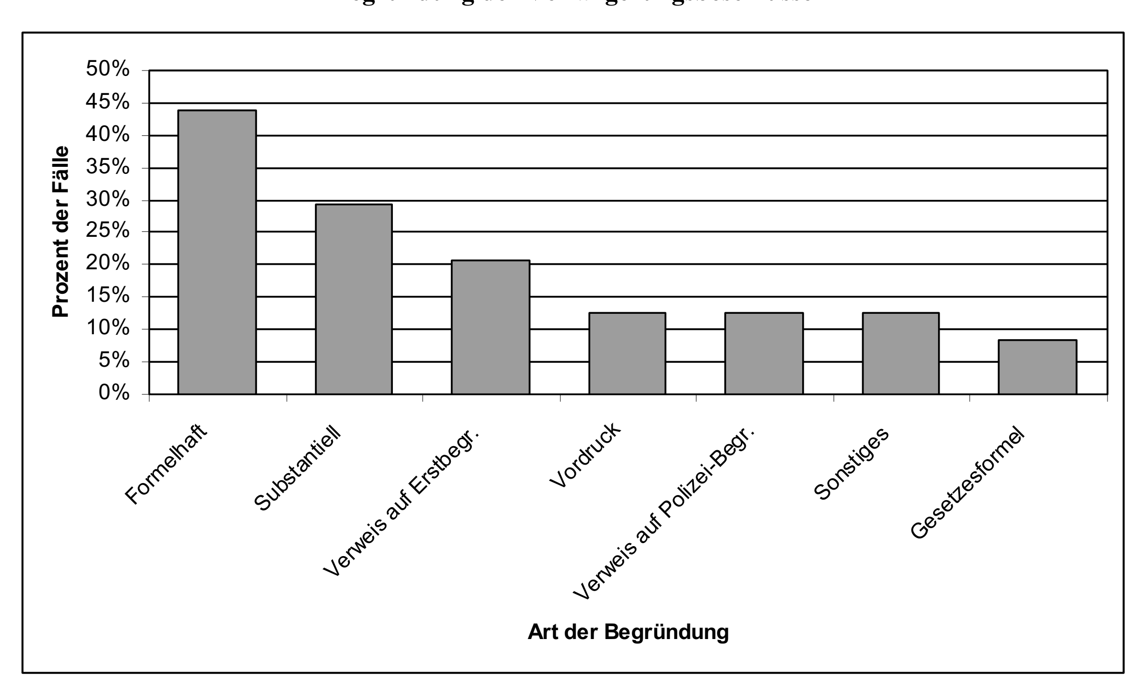


Abbildung 62

Begründungen der Polizei differenziert nach Katalogdelikten

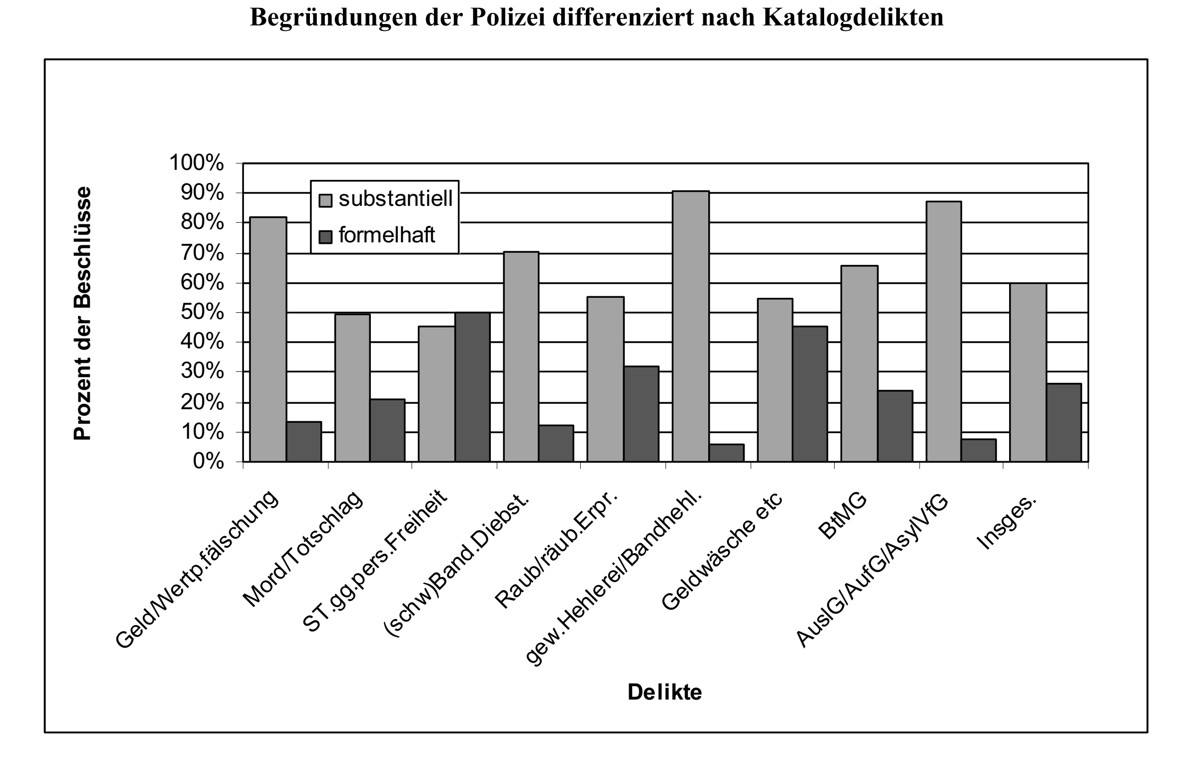
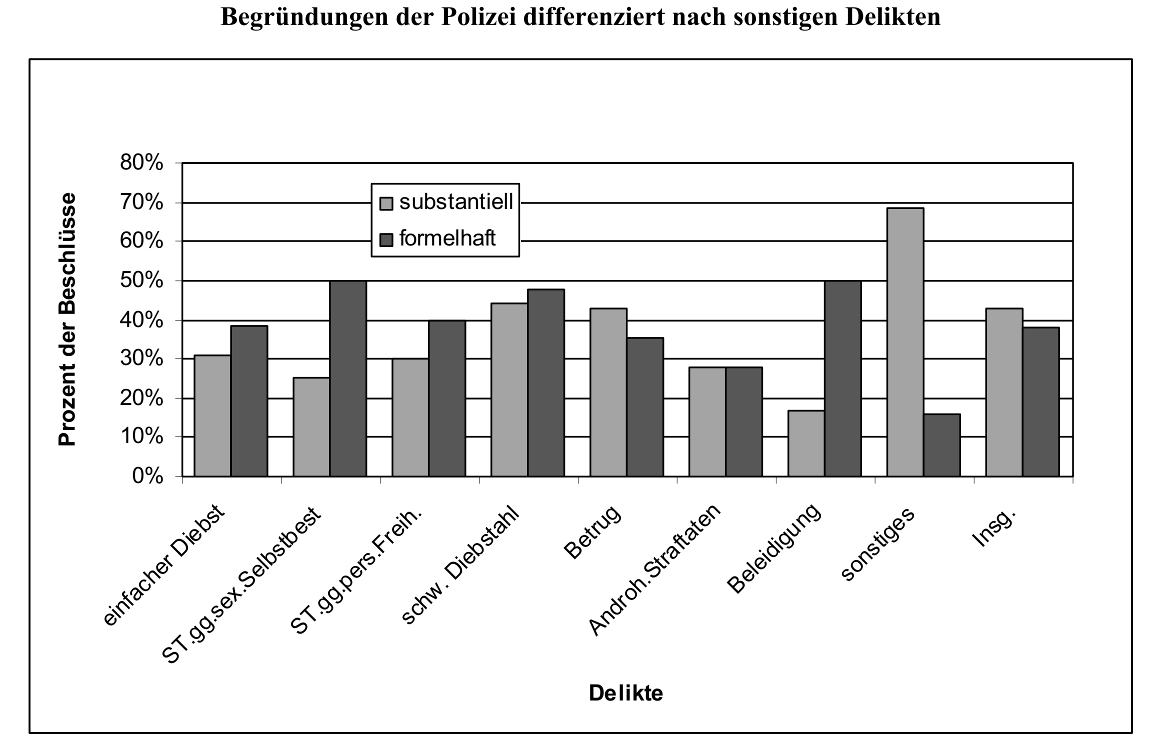


Abbildung 63

Begründungen der Polizei differenziert nach sonstigen Delikten



Bei den sonstigen Delikten waren Anregungen der Polizei zur Durchführung von Verkehrsdatenabfragen wegen schwerer Diebstahlsdelikte und Betrugsdelikte am substantiellsten begründet, lagen aber noch unter dem Durchschnitt der Katalogdelikte. Die formelhaftesten Begründungen wurden bei Straftaten gegen die sexuelle Selbstbestimmung (mittels Endeinrichtung), Beleidigungen und wiederum schweren Diebstählen festgestellt.

Eine ähnliche Verteilung von substantiellen und formelhaften Begründungen auf Katalog- und sonstige Delikte ist auch bei den staatsanwaltschaftlichen Anträgen und Eilanordnungen zu bemerken. Bei zugrundeliegenden Katalogdelikten überwiegen die substantiellen Begründungen (Abbildung 64), vor allem bei Geldwäsche, gewerbsmäßiger (Banden-) Hehlerei und Verstößen gegen das Ausländerrecht.

Bei den sonstigen Delikten dagegen sind die Begründungen der Staatsanwälte überwiegend formelhaft (27 Prozent, Abbildung 65). Nur bei Straftaten gegen die sexuelle Selbstbestimmung überwiegen die substantiellen Begründungen. Vor allem bei einfachen Diebstählen und Betrugsdelikten sind formelhafte Begründungen zu verzeichnen, wobei bei letzteren auch die substantiellen Begründungen 32 Prozent ausmachen.

Abbildung 66 zeigt die Qualität der Begründungen durch die Richter für die Anordnungen der Verkehrsdatenabfrage in Bezug auf die einzelnen Katalogdelikte.

Die Begründungsqualität bei den Katalogdelikten sinkt von der Polizei (substantiell: 60 Prozent), über die Staatsanwaltschaft (substantiell: 37 Prozent) zu den Richtern, bei denen nur noch 26 Prozent substantiell begründet sind.

Ausführliche Begründungen sind bei zugrundeliegenden Verstößen gegen das AuslG bzw. AufenthG festzustellen. Auch noch überdurchschnittlich gut begründet werden Tötungs-, Betäubungsmittel- und Geldwäschedelikte. Bei Geld- und Wertpapierfälschungen, Raub- und räuberischer Erpressung sowie Straftaten gegen die persönliche Freiheit sind die Begründungen dagegen überwiegend formelhaft.

Bei den sonstigen Delikten überwiegen auch bei den Richtern wie schon bei den Staatsanwälten die formelhaften Begründungen (Abbildung 67). Vor allem bei einfachen Diebstählen, Androhungen von Straftaten und Beleidigungen wurden die Beschlüsse nach §§ 100g, 100h StPO formelhaft begründet. Überwiegend substantielle Begründungen gab es bei Straftaten gegen die persönliche Freiheit und bei Betrug.

Abbildung 64


Begründungen der StA differenziert nach Katalogdelikten

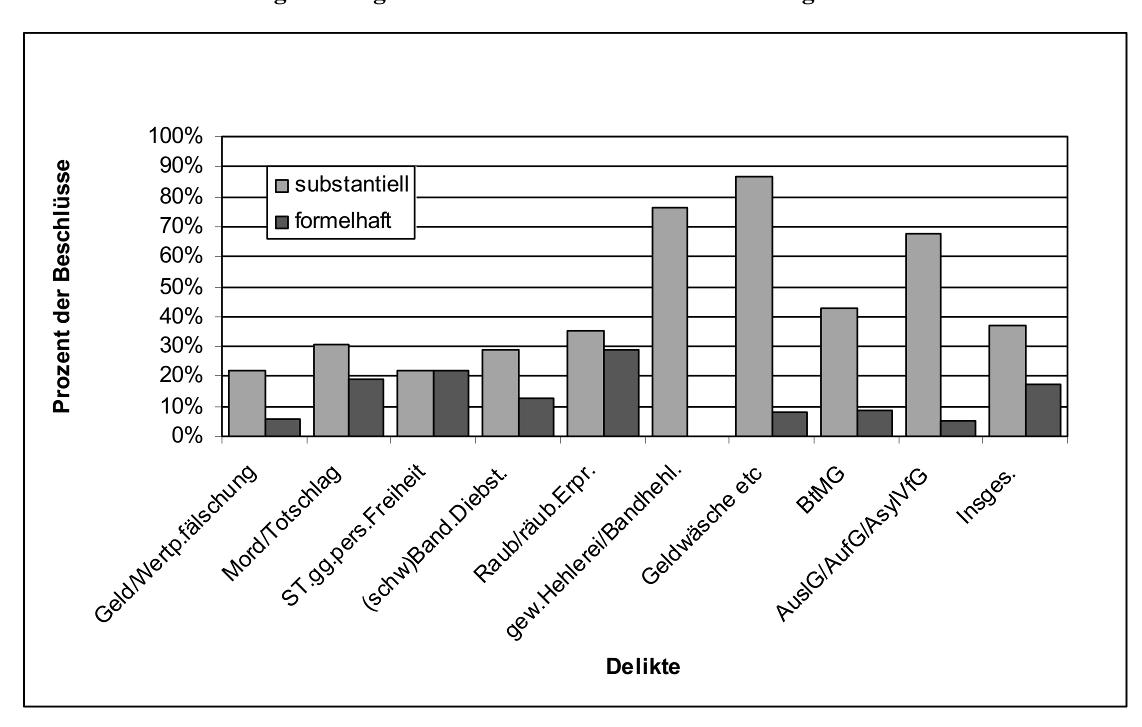


Abbildung 65

Begründungen der StA differenziert nach sonstigen Delikten

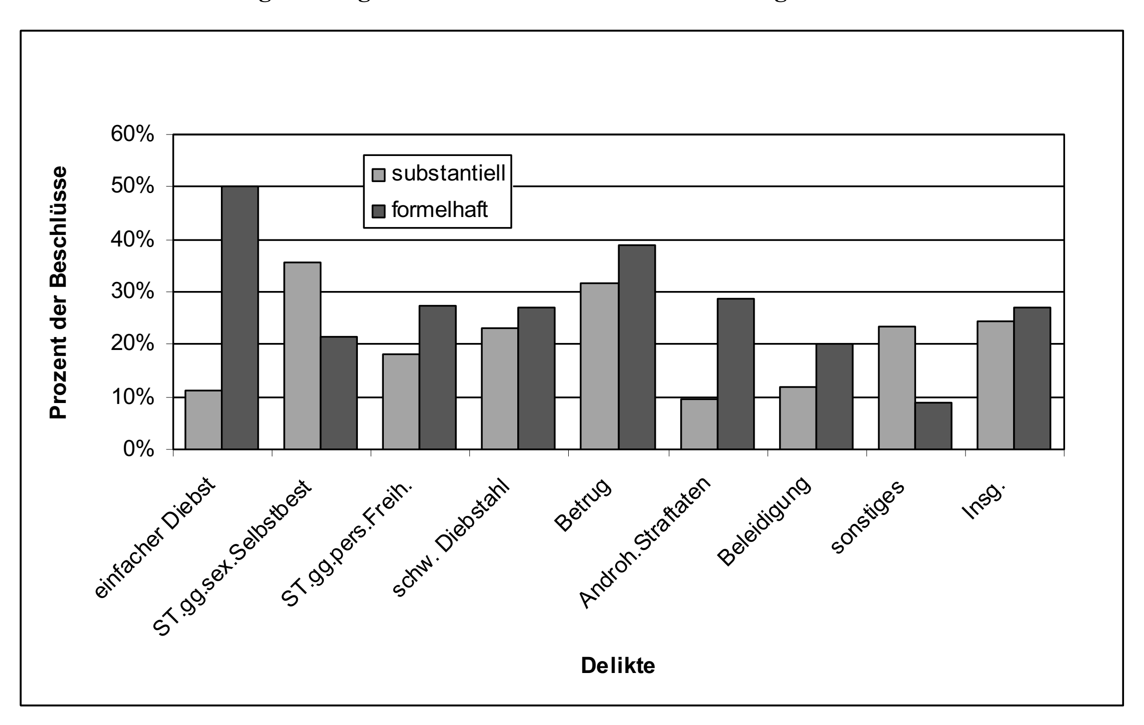


Abbildung 66

Begründungen des Gerichts differenziert nach Katalogdelikten

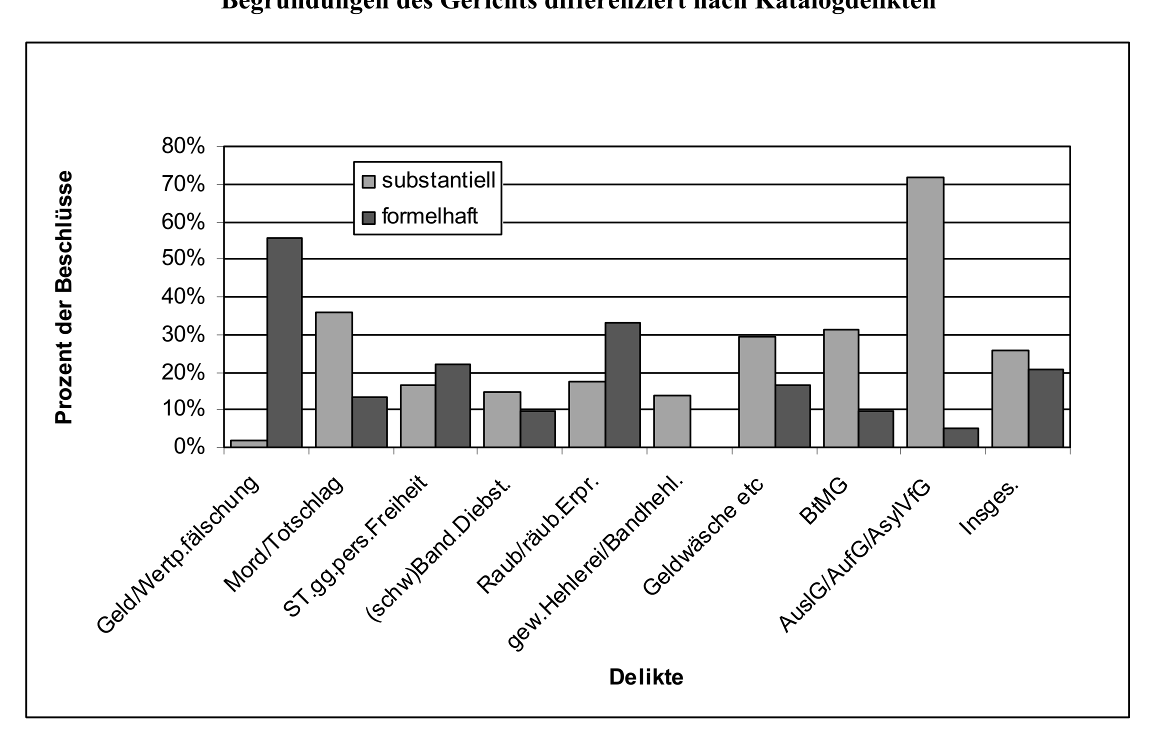
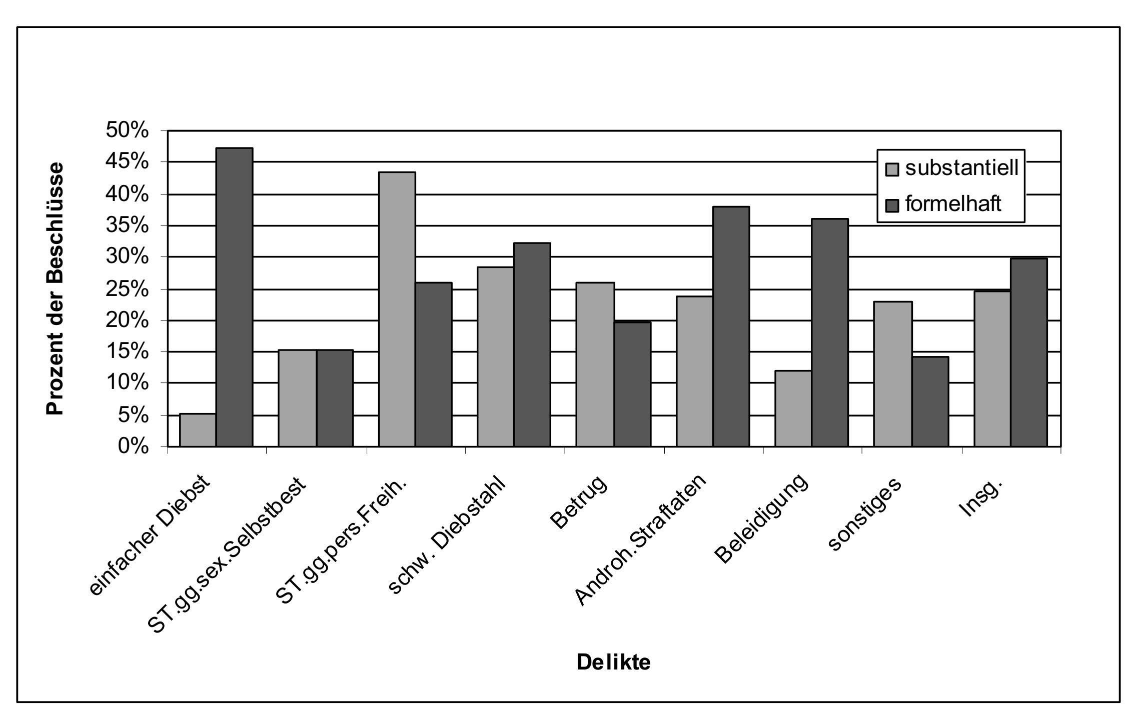


Abbildung 67



Begründungen des Gerichts differenziert nach sonstigen Delikten



3. Experteninterviews

Im Rahmen der Expertengespräche wurden Fragen zur Begründung der Anträge und Anordnungen sowie allgemein zum Richtervorbehalt gestellt.

a) Polizeibeamte

(1) Zeitlicher Aufwand für die Prüfung der Voraussetzungen

Der zeitliche Aufwand für die Prüfung der rechtlichen Voraussetzungen der Verkehrsdatenabfrage wurde von den meisten Befragten als gering bezeichnet. Es handle sich um eine Standardmaßnahme, die mittlerweile regelmäßig eingesetzt werde. Es handle sich um einen reinen Routinevorgang. Gerade im Bereich der Rauschgiftkriminalität und der organisierten Kriminalität seien die Voraussetzungen, insbesondere die Erheblichkeit der Straftaten meist gegeben. Der Zeitaufwand für eine Prüfung wurde mit zwei Minuten, fünf bis zehn Minuten, 15 Minuten und einer Stunde angegeben. Einige der befragten Polizeibeamten sind allerdings der Ansicht, dass der konkrete Zeitaufwand von dem Fall bzw. dem Verfahren abhänge. Man müsse begründen, ob Telekommunikation eine Rolle gespielt habe. Die rechtlichen Voraussetzungen und die technischen Möglichkeiten müssten geprüft werden. Beim Raub von Mobiltelefonen sei dies einfach, bei Einbruchsdiebstählen dagegen sei der Nachweis der Telekommunikation schwierig. Bei Computerkriminalität bestehe nur ein minimaler Zeitaufwand, da es in diesen Fällen regelmäßig keine andere Möglichkeit gebe, Verdächtige zu ermitteln. Da es sich um einen recht geringen Eingriff handle, falle die Prüfung relativ knapp aus. Schwierig sei die Begründung nur dann, wenn mehrere Personen verdächtig und die Beteiligungsstrukturen unklar seien. Generell sei es einfacher, wenn bereits eine prozessuale Maßnahme stattgefunden habe und nun eine Folgemaßnahme angeordnet werden soll. Dann wurde ja bereits der Sachverhalt und eine Begründung geschrieben.

(2) Beibehaltung des Richtervorbehalts

Fast alle der befragten Polizeibeamten befürworten die Beibehaltung des Richtervorbehalts. Begründet wird dies damit, dass es sinnvoll sei, dass eine unabhängige Kontrollinstanz die Rechtsmäßigkeit überprüft. Aus verfassungsrechtlicher Sicht sei der Richtervorbehalt notwendig, da Artikel 10 GG ein sehr hohes Rechtsgut sei. Es handle sich um sensible Daten und es seien auch viele Unbeteiligte betroffen. Die Eingriffsintensität sei einigermaßen hoch. Weiter wurde angegeben, dass man als Ermittler selbst den „Tunnelblick“ habe. Der Richter habe diesen nicht, weil er nicht in den Ermittlungen stecke. Im Allgemeinen haben die Befragten auch in der Praxis keine Probleme mit dem Richtervorbehalt, wie z. B. lange Zeitverzögerungen: „Wenn es schnell gehen muss, geht es auch schnell“. Bei Eilbedürftigkeit bestehe die Möglichkeit der Eilanordnung. Nur ein Befragter gibt an, dass der Richtervorbehalt in Einzelfällen störe. Man erreiche den

Richter oft nicht und müsse dann dokumentieren, was man versucht hätte, um ihn zu erreichen, damit Gefahr im Verzug angenommen werden kann. Ein anderer Befragter ist der Ansicht, dass es sich bei rückwirkenden Daten um einen eher geringfügigen Grundrechtseingriff handle, für den der Richtervorbehalt nicht notwendig sei. Ein weiterer Befragter meint, dass bei §§ 100g, 100h StPO in einigen Fällen die Anordnungsbefugnis der Staatsanwaltschaft eine hinreichende Kontrolle sei. Einer der Befragten, der den Richtervorbehalt für sinnvoll hält, gibt dagegen an, dass er die faktische Umsetzung als problematisch empfindet. Der Richtervorbehalt habe nicht mehr als eine „Alibifunktion“. Die Richter könnten aus zeitlichen Gründen nicht die gesamte Akte lesen und prüfen. Einer der Befragten findet, der Richtervorbehalt sollte abgeschafft werden. Er sei überwiegend wirkungslos. Der Richter verlasse sich auf die Informationen der Polizei und es entstehe nicht der Eindruck, als würde er sich in die Ermittlungen hineinversetzen.

b) Staatsanwälte

(1) Begründung des Antrags bzw. des Beschlusses

Die Staatsanwälte wurden darüber befragt, wer den Beschluss tatsächlich begründet. Über die Hälfte der Befragten (insbes. Staatsanwälte aus Nordrhein-Westfalen und Berlin) berichteten, dass der Beschluss grundsätzlich vom Richter begründet werde. Die Polizei schildere in einem Vermerk den Sachverhalt und die erhoffte Wirkung der Maßnahme. Die Begründung des Antrags formuliere die Staatsanwaltschaft oder sie verweise auf die Begründung der Polizei. Der Antrag sei dabei weitgehend so gestaltet, dass er dem Beschluss entspricht. Die sei eine Arbeitserleichterung für den Richter. Diese Begründung werde dann teilweise vom Richter übernommen. Sie könne aber auch von der Begründung im Antrag abweichen. Der Richter überprüfe den Antrag und formuliere den Beschluss dann selbst. Ein Befragter führt dazu aus, dass er dies aus rechtsstaatlichen Gründen für geboten halte. Sonst sei nicht zu erkennen, ob die Begründung auf eigenständigen Überlegungen des Richters beruhe. Dagegen schilderten Staatsanwälte aus Baden-Württemberg, dass die Staatsanwaltschaft den Beschluss begründe. Die Beschlüsse würden von der Staatsanwaltschaft vorbereitet. Der Richter unterschreibe den Beschluss und übernehme die vorformulierte Begründung regelmäßig. Juristisch gesehen sei diese Begründung aber dem Richter zuzuordnen, erklärt einer der Befragten. Teilweise formulieren aber auch Staatsanwälte in Nordrhein-Westfalen und Mecklenburg-Vorpommern den Beschluss und übersendeten ihn mit dem Antrag an das Gericht, den beiliegenden Beschluss zu erlassen. Manche Richter würden die Begründung dann so übernehmen, wenn sie es zutreffend finden, andere formulierten die Gründe um. Der Beschluss werde von der Staatsanwaltschaft ausführlich begründet. Das sei von der persönlichen Präferenz der Richter abhängig. Einer der Befragten gab an, sich dadurch selbst zu kontrollieren und dem Richter die Arbeit zu erleichtern. Ein anderer meint, je nachdem, ob ein Richter aus dem Eildienst (wechselnde Richter) oder ein Ermittlungsrichter die Maßnahme anordne, formuliere er die Beschlüsse vor, da erstere meist wenig Erfahrung damit hätten.

(2) Zeitlicher Aufwand für die Prüfung der Voraussetzungen

Die Frage, wie viel Zeit für die Prüfung der Anregung Staatsanwälte investieren bzw. wie viel Zeit zur Verfügung steht, wurde unterschiedlich beantwortet. Die meisten Befragten gaben an, dass dies vom Einzelfall abhänge und nicht anders als bei anderen Maßnahmen sei. Es komme auf den Umfang der Akten an und darauf, ob es sich um einen einfachen oder komplexeren Fall handelt. Die Anträge würden selten isoliert gestellt, sondern gingen mit Durchsuchung oder Haftbefehlen einher. Es wurden Zeiten von ein paar Minuten bis zu mehreren Stunden angegeben. Die meisten Befragten gaben bis zu einer halben Stunde Zeitaufwand an.

(3) Zur Verfügung gestellte Unterlagen

In der Regel wird den Staatsanwälten zur Überprüfung des Antrags die komplette Akte zur Verfügung gestellt. Ein Befragter führt dazu aus, dass er die Bearbeitung sonst ablehne. Der gesamte Akteninhalt spiele bei der Bewertung eine Rolle. Nur bei Eilbedürftigkeit gebe es Ausnahmen, wenn die Speicherfrist sonst ablaufe. Dann würden lediglich Auszüge per Fax geschickt. Zudem gebe es Doppelakten. Bei telefonischem Eildienst erfolge eine telefonische Sachverhaltsschilderung. Weiter wurde angegeben, dass aber die gesamte Akte geschickt werde, wenn es sich um größere oder länger andauernde Verfahren handle. Es seien trotzdem detaillierte Informationen der Polizei enthalten (Anzeigenaufnahme, Zeugenvernehmungen). Bei längeren Verfahren kenne man den Sachverhalt und lasse sich nur über den neuen Sachstand informieren. Auch der Richter, der immer derselbe in einem Verfahren sei, kenne die Akte und müsse sie nicht immer wieder bekommen, wenn eine weitere Ermittlungsmaßnahme angeordnet werden soll. Er bekomme dann ebenfalls nur die neuen Erkenntnisse mitgeteilt.

(4) Beibehaltung des Richtervorbehalts

Die meisten befragten Staatsanwälte sind der Meinung, dass der Richtervorbehalt beibehalten werden sollte. Er bedeute zwar einen erhöhten Arbeitsaufwand, der mitunter zu Zeitproblemen führe. Es handle sich aber um einen erheblichen Eingriff und sensible Daten. Darüber hinaus sei es nicht mit der Rechtssystematik zu vereinbaren, wenn der Richtervorbehalt wegfiele. Es sei zu befürworten, dass mehrere Personen an der Prüfung beteiligt sind. Ein Befragter führte aus, dass die Polizei viele Anträge nach §§ 100g, 100h StPO stelle, bei denen die Voraussetzungen nicht gegeben sind. Deshalb sei die doppelte Überprüfung sachgerecht. Von der Zeit her sei es auch kein unüberwindbares Hindernis. Wenn es schnell gehen müsse, sei eine Eilanordnung möglich. Einer dieser Befragten findet die gerichtliche Ablehnungsquote eher gering. Das könne daran liegen, dass die Staatsanwaltschaft so gut prüft, dass alle Voraussetzungen klar vorlie-

gen oder daran, dass die Richter nicht genau genug prüfen. Gerade bei Eilmaßnahmen würden viele Anträge „durchgewunken“. Die Ermittlungsrichter hätten wenig Zeit, so dass nur eine eingeschränkte Kontrolle stattfinde. Allerdings könnte es sein, dass noch mehr Maßnahmen durchgeführt werden würden, wenn es den Richtervorbehalt nicht gebe. Die richterliche Kontrolle sei ein Schutz vor Missbrauch. Der Richtervorbehalt solle beibehalten, aber die Möglichkeit der Datensicherung durch die Staatsanwaltschaft eingeführt werden. Die Eilkompetenz der Staatsanwaltschaft sollte zudem gestärkt werden. Wenn der Richter mit einem Anruf nicht erreicht werden könne, sollte dies für eine Eilanordnung reichen.

Dagegen plädieren einige andere dafür, dass der Richtervorbehalt entfallen solle. Das Bewusstsein der Staatsanwaltschaft, dass sie in Rechte anderer eingreifen, sie ausreichend ausgeprägt und die Kontrolle gegenüber der Polizei effektiv. Bei weitem nicht alles, was die Polizei anrege, beantrage die Staatsanwaltschaft auch. Das, was beantragt werde, würde zu fast 100 Prozent bewilligt. Man könne das in die Richtung auslegen, dass die Richter nicht ausreichend kontrollieren. Der Richtervorbehalt sei unnötig, da eine richterliche Prüfung letztendlich nicht stattfinde. Der Richter unterschreibe einfach. Daher sei der Richtervorbehalt faktisch eine reine Formalie. Die Staatsanwaltschaft habe das gleiche rechtsstaatliche Gewissen wie der Richter. Ein Staatsanwalt ist sogar der Ansicht, dass die Prüfung durch die Polizei ausreichen würde. Eine Prüfung durch Staatsanwaltschaft und Gericht erschwere nur die Ermittlungen.

c) Richter

(1) Begründung des Beschlusses

Der Beschluss wird nur nach Angabe eines Ermittlungsrichters aus Nordrhein-Westfalen ausschließlich vom Richter begründet. Die Staatsanwaltschaft fasse den Sachverhalt im Antrag zusammen, aber die Gründe schreibe er selbst. Er bekomme keinen Entwurf des Beschlusses, den er nur noch unterschreiben müsse. Richter aus Berlin und Baden-Württemberg gaben an, dass sie eine vorformulierte Beschlussvorlage von der Staatsanwaltschaft bekämen. Sie würden sich die Beschlussbegründung ansehen und unterschreiben, wenn sie sie für richtig hielten. Nach Angabe von Befragten aus Nordrhein-Westfalen, Mecklenburg-Vorpommern und Berlin gibt es keine einheitliche Praxis. Grundsätzlich würden sie zwar die Gründe selbst schreiben. Manchmal bekämen sie aber auch eine Beschlussvorlage, die sie nur noch unterschreiben müssten oder zumindest eine von der Staatsanwaltschaft vorgegebene Begründung. Einer von diesen Richtern formuliert die Gründe zu 50 Prozent selbst. zwei der befragten Richter gaben ausdrücklich an, dass sie sich am Antrag orientieren. Ein Richter sagte, dass es vorgekommen sei, dass Staatsanwälte Anträge stellen, in dem sie nur auf einem Formular den entsprechenden Fall ankreuzen. Er habe dann auf die Begründungspflicht hingewiesen. Die Strafprozessordnung enthalte für Ermittlungsrichter ein Antragserfordernis, d. h. der Beschluss ergehe nur auf Antrag. Die Staatsanwaltschaft müsse den Antrag konkret formulieren und dem Gericht wenig Spielraum lassen. Das Gericht habe eine Kontrollfunktion und dürfe keinen Ermessensspielraum haben.

(2) Zeitlicher Aufwand für die Prüfung der Voraussetzungen

Drei der befragten Ermittlungsrichter, die (teilweise) einen Beschlussentwurf bekommen, sind der Ansicht, dass es ihnen zeitlich möglich sei, die Gründe für den Beschluss selbst zu schreiben. Zwei dieser Befragten geben dazu einschränkend an, dass dies möglich sei, wenn die personellen und sachlichen Mittel dafür vorhanden seien. Es sei zeitlich möglich, da man – wie die Staatsanwaltschaft auch – vorformulierte Word-Dokumente verwenden könne. Es wäre aber eine erhebliche Mehrbelastung und unökonomisch, immer wieder die Beschlüsse neu zu formulieren. Das System sei zwischen den Beteiligten eingespielt. Die Gründe würden entsprechend den Wünschen des jeweiligen Richters formuliert. Der Zeitaufwand für das Verfassen eines Beschlusses wird unterschiedlich beschrieben. Teilweise wurde ausgeführt, dass die Bearbeitung nur ein paar Minuten dauere, da meist kaum Erkenntnisse vorliegen. Teilweise wurde erläutert, dass es bei organisierte Kriminalität-Sachen auch mehrere Tage dauern könne.

(3) Zur Verfügung gestellte Unterlagen

Zur Prüfung des Antrags werde ihnen grundsätzlich die gesamte Akte zur Verfügung gestellt, geben alle befragten Ermittlungsrichter an. Ein Richter meinte, er weigere sich sonst, den Beschluss zu erlassen. Ausnahmen gebe es dann, wenn gerade ein Beschluss erlassen wurde und sich wenig später die Rufnummer ändere. Dann erhalte man nur Auszüge. Ebenso sei es bei Folgeanträgen. Dazu werde dann der neue Sachverhalt geschildert. Weiter wurde angegeben, dass man auch in Eilfällen ab und zu nur Auszüge bekäme. Ein befragter Richter aus Nordrhein-Westfalen ist der Ansicht, dass der Antrag allein nie ausreiche. Dagegen meint ein Befragter aus Baden-Württemberg, dass in Eilfällen auch mal nur der Antrag der Polizei und der Staatsanwaltschaft mitgeschickt würde. Ein weiterer Befragter (Mecklenburg-Vorpommern) ist der Ansicht, dass bei Folgeanträgen auch eine telefonische Absprache und ein Vermerk ohne weitere Begründung ausreichen würden.

(4) Beibehaltung des Richtervorbehalts

Alle befragten Richter sind der Ansicht, dass der Richtervorbehalt beibehalten werden sollte. Er sei wichtig und aufgrund der Vielzahl der Betroffenen geboten. Zur Begründung wird zudem auf die Erheblichkeit des Grundrechtseingriffs und die Heimlichkeit der Maßnahme verwiesen. Die Prüfung der Verhältnismäßigkeit der Maßnahme müsse durch einen Richter erfolgen. Die Kontrolle durch eine zweite Instanz (neben der Staatsanwaltschaft) sei sinnvoll. Polizei und Staatsanwaltschaft seien zwar in der Lage, aufgrund ihrer Ausbildung vieles selbständig durchzuführen. Die Funktion der Strafverfol-

gungsbehörden sei aber eine andere als die des Gerichts. Erstere würden zielorientiert arbeiten und wollten Taten aufklären. Der Ermittlungsrichter setze Grenzen. Es finde bereits vor Beantragung eine Zensur im Kopf der Polizei und Staatsanwaltschaft statt. Sie würden nichts beantragen, von dem sie wissen, dass der Richter es ablehnen würde. Schließlich sei auch nach außen hin wichtig, dass es ein Kontrollorgan gebe, das nicht in die Ermittlungen integriert ist. Die Entscheidungsvorgänge würden dadurch transparenter und die Verfahrensverläufe in den Beschlüssen besser dokumentiert. Ein befragter Richter war der Ansicht, dass bei den Richtern, die nur noch einen Beschlussentwurf unterschreiben müssen und ihre Prüfungsverpflichtung darin sehen, eine Unterschrift zu leisten, der Richtervorbehalt nur noch eine Farce sei. Andererseits seien viele Anträge einfach sehr gut begründet. Ein weiterer Richter meint einschränkend, dass der Richtervorbehalt nicht bei allen Arten der Verkehrsdatenabfrage erforderlich sei. Wenn es beispielsweise darum gehe, der IP-Adresse einen Namen zuzuordnen, halte er den Richtervorbehalt für unnötig. Das sei kein gravierender Eingriff. Dagegen sei der Richtervorbehalt etwa bei der Erstellung eines Bewegungsbildes notwendig.

d) Verteidiger

(1) Begründung der Anordnungen

Ein ganz anderes Bild der Begründungspraxis zeigen hingegen die befragten Verteidiger auf. Alle von uns Befragten halten die Beschlüsse nach §§ 100g, 100h StPO für nicht ausreichend begründet. Es würden Katalogtaten herangezogen, um eine Anordnung zu rechtfertigen, die jeweiligen Merkmale in der Begründung dann aber nicht subsumiert. Die Gerichte würden nach Angaben eines Befragten die exakte Begründung umgehen, da sie sich nicht richtig mit den Vorschriften auskennen.

(2) Beibehaltung des Richtervorbehalts

Alle befragten Rechtsanwälte sind der Meinung, dass der Richtervorbehalt beibehalten werden sollte. Wünschenswert sei aber vor allem auch, dass er ausgebaut und präzisiert werde. In der Praxis sei der Richtervorbehalt derzeit nicht besonders hilfreich. Die Befragten gaben teilweise an, dass die Polizei die Anregung schreibe, die Staatsanwaltschaft den Antrag und der Richter „nicke“ die Sache dann nur noch ab. Er unterschreibe einfach. Er habe auch gar keine Zeit, um alle notwendigen Punkte zu prüfen. Die Studien zu §§ 100a, 100b StPO hätten die Defizite aufgezeigt und dasselbe gelte auch für §§ 100g, 100h StPO. Es finde eine Entwicklung in Richtung „Big Brother“ statt. Der Richtervorbehalt stelle nach Ansicht eines Befragten aber immerhin eine psychologische Hemmschwelle für Polizei und Staatsanwaltschaft dar. Die Tatbestandsvoraussetzungen sollten jedoch strenger sein. Die Novelle des BMJ habe den Richtervorbehalt nach Ansicht eines Befragten nicht so präzisiert, wie es notwendig gewesen wäre. Die Begründungspflicht sollte präzisiert, der Katalog begrenzt und damit der präventive Grundrechtsschutz gestärkt werden. Vorgeschlagen wurde z. B., eine Begründungspflicht für die Zustimmung zu einem Beschluss einzuführen, jedoch darauf zu verzichten für die Ablehnung des Beschlusses.

e) Telekommunikationsunternehmen

Der Großteil der Anordnungen entfällt nach Angaben von vier der befragten Unternehmen auf richterliche Beschlüsse (zwischen 85 Prozent und 98 Prozent) und nicht auf staatsanwaltschaftliche Eilanordnungen. Ein Befragter gibt an, dass er dabei regionale Unterschiede beobachtet habe. Die Situation variiere auch je nach Rechtsprechung zur Abfrage von Personendaten zu dynamischen IP-Adressen.

f) Datenschützer

(1) Begründung der Anordnungen

Auch bei den befragten Datenschützern herrscht der Eindruck vor, dass die Vorraussetzungen der Anordnungen inhaltlich nicht sorgfältig genug geprüft würden. Sie berichten von Fällen, in denen sich der Eindruck aufdränge, dass gar kein Tatverdacht vorliegt und die Polizei die Anordnung anregt, um herauszufinden, ob die Straftaten, die eine Anordnung begründen würden, überhaupt vorliegen. Mitunter sei auch unklar, welche Unterlagen dem Anordnenden überhaupt zur Verfügung gestellt würden und wie sorgfältig die Voraussetzungen geprüft würden.

(2) Beibehaltung des Richtervorbehalts

Alle befragten Datenschützer sprechen sich nicht nur für die Beibehaltung des Richtervorbehalts, sondern auch für dessen Verbesserung und Stärkung aus. Er sei im Hinblick auf seine grundrechtsschützende Funktion von eminenter Bedeutung. Als Begründung wurde u. a. angeführt, dass gerade wegen der Heimlichkeit der Maßnahme eine unabhängige Kontrolle durchgeführt werden müsse. Richter würden den Grundrechten ein anderes Gewicht beimessen als Ermittlungsbeamte, die unter Effektivitätsgesichtspunkten handeln. Alle befragten Datenschutzbeauftragten äußerten allerdings Zweifel an der tatsächlichen Umsetzung des Richtervorbehalts bzw. daran, ob der Richtervorbehalt momentan wirklich seine Funktion erfülle. Die Qualität der Prüfung durch den Richter sei oft nicht sehr hoch. Beschlüsse seien häufig genauso formuliert wie der Antrag der Staatsanwaltschaft. Auch sei unklar, ob die Ermittlungsakte überhaupt gelesen werde oder ob der Richter nur die Begründung der Staatsanwaltschaft sehe und sich damit zufrieden gebe. Das sei völlig unzureichend. Der Richtervorbehalt müsse daher als Sicherungsmaßnahme so gestärkt werden, dass er seine Funktion tatsächlich erfüllen kann.

4. Zusammenfassung der Ergebnisse

Sowohl durch die mündliche und schriftliche Befragung als auch durch die Aktenanalyse konnte festgestellt werden, dass der Großteil der Anordnungen von den Ermittlungsrichtern erlassen wird. Im Mittel wurde bei den schriftlich befragten Staatsanwälten geschätzt, dass die Anordnungen zu 87 Prozent durch den Richter erfolgen.

Die Auswertung der Akten ergab, dass 90 Prozent der Verkehrsdatenabfragen gerichtlich angeordnet wurden. Auch die interviewten Telekommunikationsanbieter schätzten die richterliche Anordnungsquote mit 90 Prozent sehr realistisch ein. Richterlich bestätigt werden Eilanordnungen nach Einschätzungen aus der schriftlichen Befragung häufig bis immer (zusammen 98 Prozent). Aus der Auswertung der Akten ergab sich, dass 69 Prozent der Eilanordnungen ausdrücklich bestätigt wurden, die Maßnahmen aber auch ohne richterliche Bestätigung größtenteils durchgeführt wurden. Ablehnungen von Anträgen sind nach den Ergebnissen der schriftlichen Befragung äußerst selten. Die schriftlich befragten Staatsanwälte gaben zu 88 Prozent an, dass Anträge selten bis nie abgelehnt werden. Aus den Akten selbst ergeben sich lediglich fünf Ablehnungen[446]. Auch nach Einschätzung der interviewten Staatsanwälte ist die Ablehnung der Anträge die absolute Ausnahme. Das könnte daran liegen, dass die Staatsanwaltschaft die unzulässigen Anregungen bereits sorgfältig prüft und selektiert oder daran, dass der Richter die Anträge nicht ausreichend prüft. Letzteres nehmen die befragten Verteidiger und Mitarbeiter der Datenschutzbeauftragten der Länder an. Teilweise wird die Einbeziehung des Richters – gerade auch von Polizei und Staatsanwaltschaft – als „reine Formsache“ bezeichnet. Der Richtervorbehalt habe hier eine Art „Alibifunktion“. Trotzdem befürworten die meisten der mündlich und schriftlich Befragten die Beibehaltung des Richtervorbehalts[447]. 61 Prozent der schriftlich befragten Staatsanwälte wollen den Richtervorbehalt nicht abschaffen und so beibehalten, wie er derzeit ausgestaltet ist. Auch die überwiegende Mehrheit der Polizeibeamten und interviewten Staatsanwälte sowie alle Richter, Verteidiger und Datenschützer geben an, dass der Richter seine Kontrollfunktion weiter ausüben solle. Die Prüfung durch ein außerhalb des Ermittlungsverfahrens stehendes Organ sei äußerst wichtig. Die befragten Strafverteidiger und Datenschützer fordern allerdings, dass der Richtervorbehalt weiter ausgebaut werden müsse, da er seine Funktion derzeit nicht erfülle.

Die Ergebnisse der Aktenanalyse zur Begründung von Anregung, Antrag und Beschluss haben gezeigt, dass die Qualität der Begründung von der Anregung durch die Polizei bis zum Erlass des Beschlusses abnimmt. Während die Polizeibegründungen in 55 Prozent der Fälle als substantiell bewertet wurden, ist dies bei der Begründung der Staatsanwaltschaft nur noch zu 34 Prozent der Fall, und die richterlichen Begründungen werden nur noch zu 25 Prozent substantiell begründet. Dabei gibt es Unterschiede entlang der Bundesländer. Baden-Württemberg fällt durch substantiell begründete Anregungen der Polizei, aber auch dadurch auf, dass die Staatsanwaltschaft hier dem Richter größtenteils Beschlussentwürfe zur Unterschrift mitschickt. Dadurch ist der Anteil an richterlichen Begründungen, die wortgleich wie der Antrag der Staatsanwaltschaft ausgeführt sind, sehr groß. Berlin weist ebenfalls einen großen Anteil an substantiell begründeten Anregungen der Polizei auf, wobei jedoch auch sehr häufig der Wortlaut des Gesetzes zitiert wird. Bei den Begründungen der Anträge durch die Staatsanwälte überwiegen dann die formelhaften Begründungen, wobei das häufige Verwenden der Gesetzesformeln einer der Hauptgründe dafür ist, da dies besonders häufig vorkam und die Wiedergabe des Gesetzestextes unter „formelhaft“ eingeordnet wurde. Diese Zitierung der Gesetzesformulierungen überwiegt dann schließlich auch bei den gerichtlichen Begründungen in Berlin, wobei ein Großteil der Beschlüsse so formuliert ist wie der Antrag der Staatsanwaltschaft. Da Mehrfachnennungen möglich waren, wird das häufige Vorkommen der Gesetzesformulierungen meist darauf beruhen, dass die Anträge der Staatsanwälte wortwörtlich übernommen wurden und damit auch die Gesetzesformeln. Nordrhein-Westfalen fällt durch insgesamt häufige substantielle Begründungen von der Anregung bis zum Beschlusserlass auf. Allerdings sind bei den Polizeibegründungen auch häufige formelhafte Begründungen zu bemerken und die staatsanwaltschaftlichen Begründungen verweisen etwas häufiger als in den anderen Bundesländern auf die Polizeibegründung. Bei den Beschlüssen ist der Anteil an substantiellen Begründungen und solchen, die wie der Antrag der Staatsanwaltschaft ausgeführt sind, gleich groß. In Mecklenburg-Vorpommern waren substantielle Polizeibegründungen festzustellen, während bei den staatsanwaltschaftlichen Begründungen die formelhaften überwogen. Zudem war die Zusendung von Beschlussentwürfen hier wiederum häufiger. Die gerichtlichen Begründungen sind aufgrund der häufigen Verwendung von Gesetzesformeln überwiegend formelhaft. Zudem ist ein großer Teil wie der Antrag der Staatsanwaltschaft ausformuliert. Bei den staatsanwaltschaftlichen Eilanordnungen nimmt die Qualität der Begründungen erwartungsgemäß ab. Vordrucke, formelhafte Begründungen und die Verwendung der Gesetzesformeln überwiegen hier länderübergreifend. Ebenso gestaltet sich das Bild bei den richterlichen Bestätigungen. Keine Begründungen, formelhafte Ausführungen und die Zitierung des Gesetzeswortlauts herrschen hier vor. Dabei fallen vor allem Mecklenburg-Vorpommern und Berlin auf. Die Zusendung von Beschlussentwürfen wird – auch in bundeslandspezifischer Hinsicht – durch die Expertengespräche bestätigt.

IV. Dauer der Maßnahmen

Im Folgenden wird die Dauer der Verkehrsdatenabfrage ermittelt. Dabei soll überprüft werden, wie lange der Abfragezeitraum ist bzw. ob es Unterschiede zwischen beantragter und angeordneter Dauer gibt.

1. Schriftliche Befragung

a) Beantragte und angeordnete Dauer

Die mittels schriftlichen Fragebogens befragten Staatsanwälte sollten den Zeitraum, für den die Abfrage der Daten in der Regel beantragt wird, angeben.

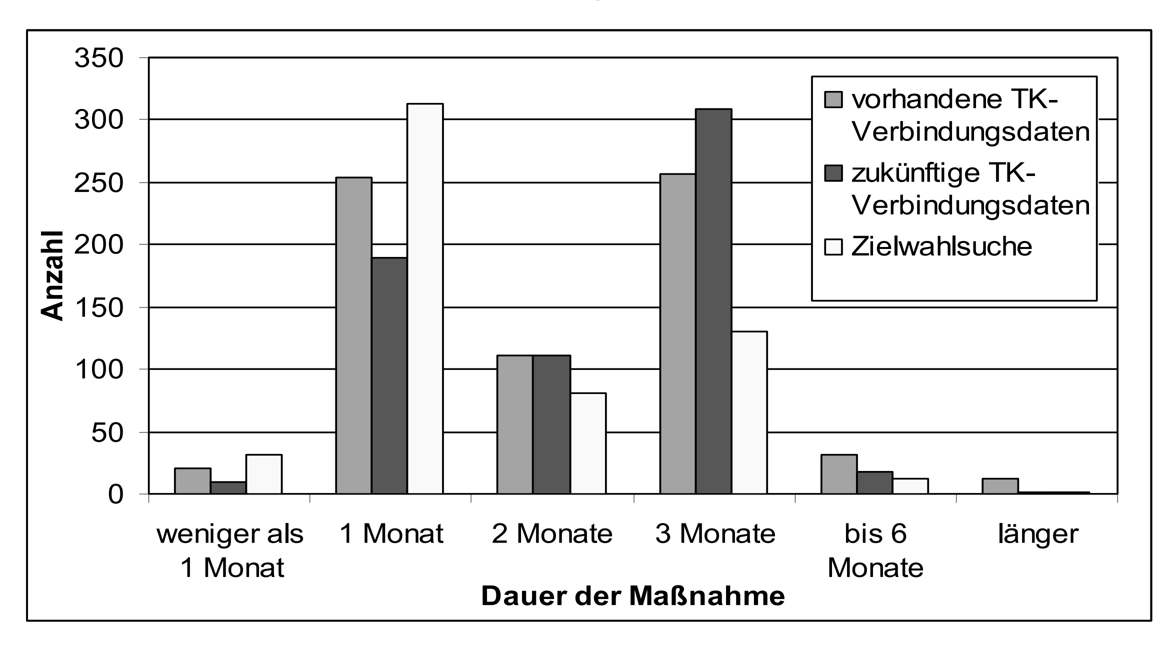
---

[446] Aufgrund des Aktenzugangs über die Netzbetreiber konnten die Ablehnungen von Anträgen nicht systematisch erfasst werden.

[447] Dies deckt sich mit den Stellungnahmen des Schrifttums, vgl. hierzu *Brüning*, 2005, S. 111ff.

Abbildung 68

Durchschnittliche beantragte Dauer der Maßnahme



Nach Einschätzung der Befragten werden die Maßnahmen nach §§ 100g, 100h StPO im Schwerpunkt für einen oder drei Monate beantragt (siehe Abbildung 68). Eine Dauer von zwei Monaten ist deutlich weniger verbreitet. Selten wird eine Dauer von weniger als einem Monat bzw. länger als drei Monaten beantragt. Dies deckt sich mit den aus den bislang vorliegenden empirischen Befunden bekannten Verteilungen. Differenziert man nach Anwendungsbereichen der Maßnahme, so gibt es kaum Unterschiede zwischen vorhandenen und zukünftigen Verkehrsdaten (durchschnittlich knapp über zwei Monate), während die Zielwahlsuche durchschnittlich für einen kürzeren Zeitraum beantragt wird (durchschnittlich einen bis zwei Monate). Die Befragten gehen davon aus, dass die angeordnete fast immer der beantragten Dauer entspricht. Wenn es Abweichungen gebe, dann tendenziell Änderungen zu kürzerer Dauer. 62 Prozent der Befragten nehmen an, dass die angeordnete und die tatsächliche Dauer der Verkehrsdatenabfrage häufig übereinstimmen. 19 Prozent der Befragten meinen, dass Anordnungsdauer und tatsächliche Dauer immer übereinstimmen.

b) Verlängerungen

Im Jahr 2005 wurden nach Einschätzung der Befragten in 40 Prozent der Fälle Verlängerungen selten bis gelegentlich beantragt. 60 Prozent gaben an, dass keine Verlängerung beantragt wurde. Abgelehnt wurden diese Verlängerungen nie (69 Prozent), selten (26 Prozent) oder gelegentlich (5 Prozent).

2. Aktenanalyse

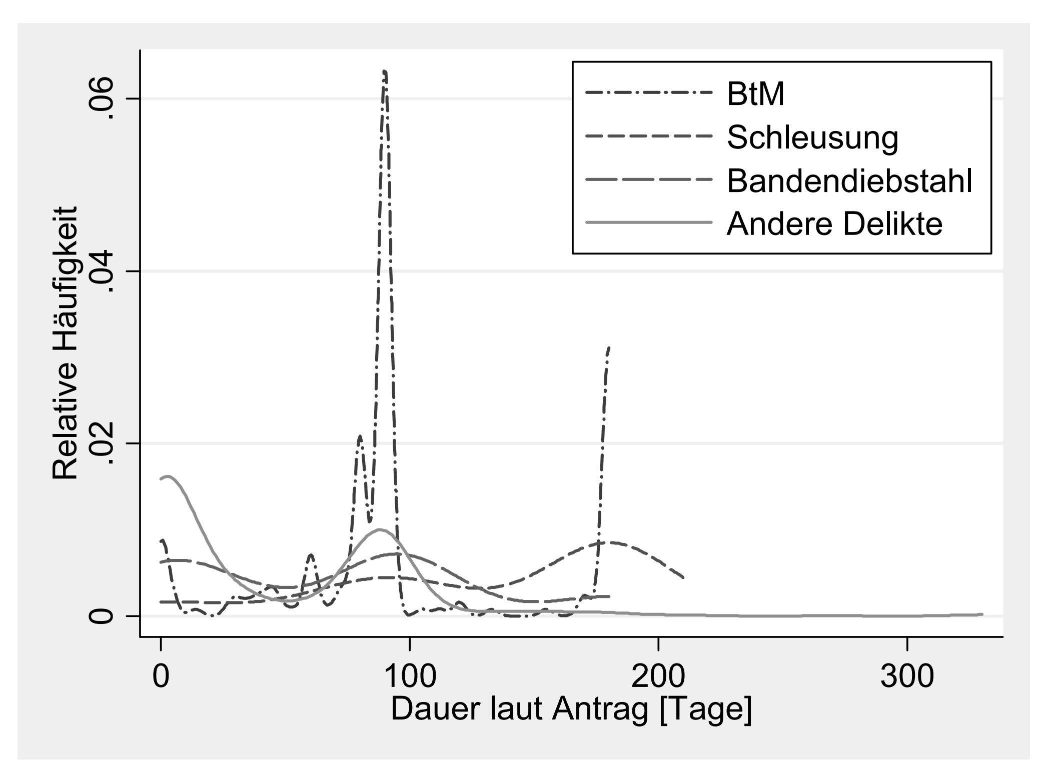
a) Dauer der Maßnahmen

In 88 Prozent der Beschlüsse betrug die Antragsdauer bis zu drei Monaten. Bei den übrigen 12 Prozent handelt es sich fast ausschließlich um sowohl in die Zukunft als auch in die Vergangenheit gerichtete Verkehrsdatenabfragen. Lediglich in fünf Fällen konnte festgestellt werden, dass eine Verkehrsdatenabfrage von zukünftigen Daten beantragt wurde, die die zulässige Höchstdauer von drei Monaten (§ 100h I Satz 3 i. V. m. § 100b II Satz 4 StPO) überschritt. Diese Abfragen waren auf 100 Tage ausgerichtet. Den 12 Prozent der Beschlüsse, mit denen über einen längeren Zeitraum als 90 Tage Daten abgefragt wurden, lagen vor allem Betäubungsmitteldelikte (42 Prozent), Schleusungen (30 Prozent) und (schwere) Bandendiebstähle (22 Prozent) zugrunde. Schwerpunktmäßig wurden bei diesen Betäubungsmitteldelikten und Schleusungen Abfragen in die Vergangenheit und in die Zukunft von insgesamt sechs Monaten beantragt, während sich die Abfragen bei den Bandendiebstählen sowohl häufig auf 100 Tage als auch häufig auf sechs Monate richteten. Bei Betäubungsmitteldelikten und Schleusungen handelt es sich um Delikte, bei denen nicht nur einmalig eine Tat begangen wird, sondern es die Regel ist, dass über einen längeren Zeitraum Geschäfte abgewickelt werden. Bandendiebstähle erstrecken sich schon per Definition über einen längeren Zeitraum. Demnach sind die Abfragezeiträume bei diesen Delikten erwartungsgemäß länger als bei anderen Delikten (siehe Abbildung 69, die alle Beschlüsse beinhaltet).

Abbildung 69



Dauer der Maßnahmen laut Antrag differenziert nach Delikten



b) Differenzierung nach der Art der Verkehrsdatenabfrage

Der Abfragezeitraum variiert je nach Art der Verkehrsdatenabfrage. Es gab Abfragen für den Zeitraum von ein paar Sekunden, aber auch von mehreren Monaten. Bei der Abfrage von vorhandenen Daten liegt die Dauer zu einem Viertel unter einem Tag. Ein weiterer Schwerpunkt ist bei drei Monaten zu bemerken (ein weiteres Viertel). Bei der Abfrage von zukünftigen Daten liegt der Schwerpunkt des Abfragezeitraums bei drei Monaten (42 Prozent). Die Zielwahlsuche erfolgt schwerpunktmäßig ebenfalls für einen Zeitraum von drei Monaten (30 Prozent) oder von unter einem Tag (25 Prozent). Sie wird also häufig nur für ein paar Stunden beantragt und angeordnet. Die beantragte Dauer wurde bei 32 Anschlüssen vom Richter verändert. In sechs Fällen wurde der Abfragezeitraum verkürzt, während er in neun Fällen verlängert wurde. In 17 Fällen wurde der Zeitraum konkretisiert. So wurde z. B. die beantragte „Abfrage zukünftiger Daten“ auf drei Monate befristet oder die „retrograden Verkehrsdaten“ auf 80 Tage festgelegt.

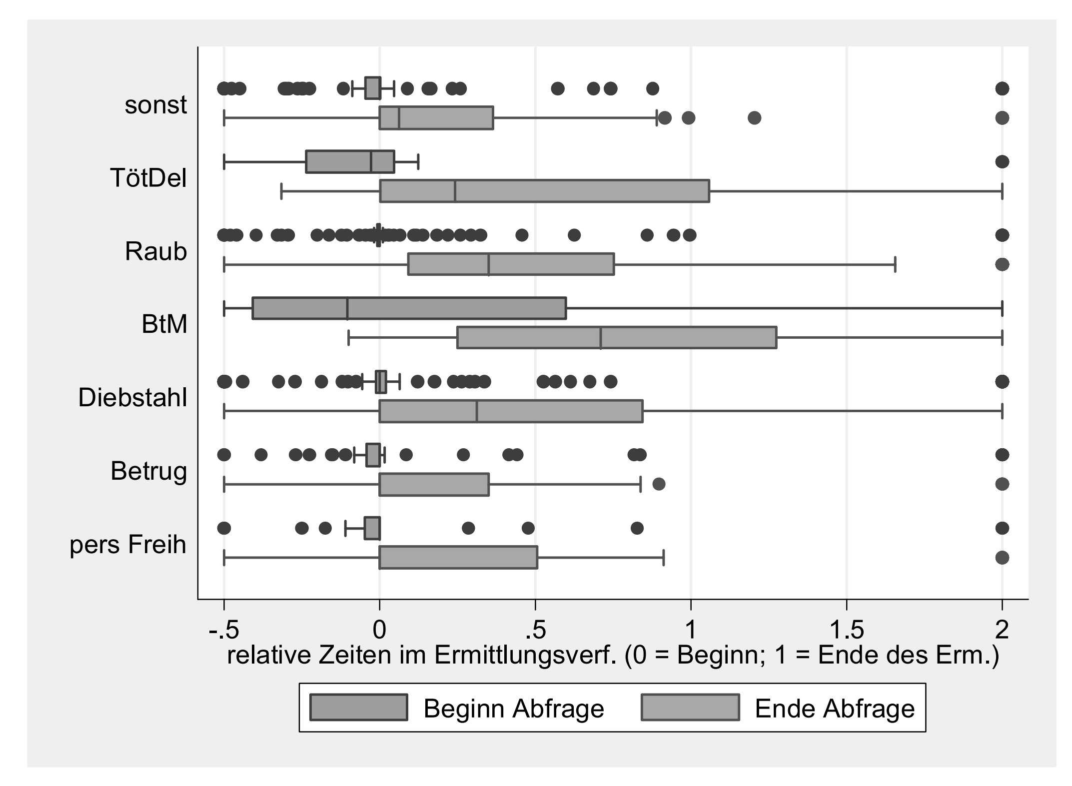
c) Deliktsspezifische Unterschiede in den Abfragezeiträumen

Wie sich der Abfragezeitraum je nach dem, welches Delikt dem Verfahren zugrunde liegt, verändert, lässt sich Abbildung 70 entnehmen. Diese Abbildung zeigt auf einer Skala von null bis eins das Ermittlungsverfahren. Als Beginn des Ermittlungsverfahrens wurde dabei die Einleitung des Ermittlungsverfahrens durch die Polizei oder – wenn dies aus den Akten nicht ersichtlich war – der Zeitpunkt der ersten Einschaltung der Staatsanwaltschaft gewählt. Als Ende des Ermittlungsverfahrens wurde aus forschungspraktischen Gründen (insoweit abweichend von § 169a StPO) der Zeitpunkt des polizeilichen Abschlussberichts oder – wenn dieser Zeitpunkt den Akten nicht zu entnehmen war – der Zeitpunkt der Anklage oder Einstellung des Verfahrens gewählt. Da es sich bei der folgenden Abbildung um den Zeitraum handelt, für den die Verkehrsdaten abfragt werden, kann der Beginn der Abfrage bei in die Vergangenheit gerichteten Abfragen vor Beginn des Ermittlungsverfahrens liegen. Bei dem Strich, der innerhalb der Boxen abgebildet ist, handelt es sich um den Median. Die sonstigen Punkte sind Ausreißer und Extremwerte. Die Striche außerhalb der Boxen markieren den Zeitraum, über den sich die Maßnahmen erstrecken. Die Kategorie „Raub“ erfasst dabei auch (räuberische) Erpressungen.

Dabei fällt auf, dass bei Tötungsdelikten und Betäubungsmitteldelikten eine Abfrage der Daten aus der Vergangenheit häufiger als bei anderen Delikten erfolgt, wobei das Ende der Abfrage fast immer in der Zukunft liegt. Für Betäubungsmitteldelikte ist anzumerken, dass Beginn

Abbildung 70

Abfragezeitraum differenziert nach Delikten



und Ende der Abfragen am weitesten auseinander liegen. Das Ende der Abfrage geht teilweise über das polizeiliche Ermittlungsende hinaus. Dabei ist jedoch zu berücksichtigen, dass es sich um den angegebenen Abfragezeitraum handelt, die Abfrage der Daten bei Vorliegen ausreichenden Beweismaterials aber abgebrochen worden sein kann. Bei den übrigen Delikten liegt der Beginn der Abfrage meist vor Beginn des Ermittlungsverfahrens und ist damit auch in die Vergangenheit gerichtet, jedoch ist dies nicht so ausgeprägt wie bei Betäubungsmittel- und Tötungsdelikten. Das Ende liegt hier meist innerhalb der ersten Hälfte des Ermittlungsverfahrens.

d) Verlängerungen

Bei 53 Beschlüssen wurden Verlängerungen des Abfragezeitraums beantragt. Alle Verlängerungsanträge wurden bewilligt. Die Verlängerungsdauer variierte zwischen einem und vier Monaten, wobei am häufigsten eine Verlängerung um drei Monate beantragt wurde (34 Beschlüsse). Am zweithäufigsten war eine beantragte Verlängerungsdauer von zwei Monaten (acht Beschlüsse). Bei fünf Beschlüssen wurde beantragt, den Beschluss um einen Monat zu verlängern. Auch hier sind keine Unterschiede zwischen Antrag und Beschluss festzustellen. Die beantragte Dauer wurde bei allen Beschlüssen bewilligt. Die Entscheidung über die Bewilligung der Verlängerung wurde von den Richtern größtenteils sofort getroffen (25 Beschlüsse). Bei sieben Beschlüssen dauerte die Entscheidung einen Tag. Bei den übrigen Verlängerungsbeschlüssen dauerte es von zwei bis zu sieben Tagen bis zur Entscheidung.

3. Zusammenfassung der Ergebnisse

Die beantragte Dauer der Maßnahmen entspricht weitgehend der angeordneten Dauer. Dies zeigen sowohl die Ergebnisse der Aktenanalyse als auch die der schriftlichen Befragung. Übereinstimmend wird durch beide Module festgestellt, dass die Abfragedauer schwerpunktmäßig bei drei Monaten liegt. Darüber hinaus ist ein weiterer Schwerpunkt bei den Abfragen innerhalb eines Tages zu bemerken. Das ergibt sich aus der Aktenanalyse und in abgeschwächter Form auch aus der schriftlichen Befragung. Zwar gaben die Befragten hier meist einen Monat als Abfragezeitraum an. Allerdings war die Kategorie „weniger als ein Monat“ im Fragebogen nicht vorgegeben. Es ist zu vermuten, dass die vorgegeben Kategorie „ein Monat“ auch häufig dann von den Befragten gewählt wurde, wenn sich die Abfrage innerhalb eines Monats bewegte. Je nach Art der Abfrage gibt es Unterschiede bei den Abfragezeiträumen. So erfolgt die Abfrage vorhandener Daten meistens für einen Zeitraum innerhalb eines Tages oder für die Dauer von drei Monaten. Bei in die

Zukunft gerichteten Abfragen werden meistens drei Monate gewählt. Die Zielwahlsuche erfolgt schwerpunktmäßig innerhalb eines Tages oder für drei Monate. Nur bei 32 von 1909 Anschlüssen, die im Rahmen der Aktenanalyse untersucht wurden, wurden Veränderungen hinsichtlich der Dauer der Abfrage durch den Richter vorgenommen, wobei in den meisten Fällen die Dauer der Maßnahme reduziert bzw. konkretisiert wurde (z. B. statt wie im Antrag auf „vorhandene Verkehrsdaten“ gerichtet, wurde die Abfrage begrenzt auf 80 Tage in die Vergangenheit gerichtet). Den geringen Unterschieden zwischen beantragter und angeordneter Dauer in den Akten entspricht auch die Einschätzung der befragten Staatsanwälte, welche größtenteils davon ausgehen, dass die angeordnete fast immer der beantragten Dauer entspricht. Aus der Auswertung der Akten ergibt sich zudem, dass der Abfragezeitraum je nach zugrunde liegendem Ermittlungsdelikt variiert. So ist vor allem bei Raub- und Tötungsdelikten der Abfragezeitraum öfter in die Vergangenheit gerichtet als bei anderen Delikten. Das wird bei Tötungsdelikten wohl daran liegen, dass zunächst festgestellt werden muss, mit wem der Getötete in Kontakt stand. Bei Raubüberfällen kann (mittels Funkzellenabfrage) überprüft werden, wer im Bereich des Tatorts vor, während und nach der Tatzeit mit anderen telefonisch in Kontakt stand. Bei Betäubungsmitteldelikten liegen Beginn und Ende der Abfrage am weitesten auseinander. Hier werden über einen längeren Zeitraum Täterstrukturen und Geschäftskreise untersucht. Verlängerungen wurden in den ausgewerteten Verfahren nur bei 53 von 1 257 Beschlüssen beantragt. Beantragte Verlängerungen wurden – nach den Ergebnissen der Aktenanalyse – immer bewilligt. Auch die schriftlich befragten Staatsanwälte schätzten, dass die Verlängerungen zu 70 Prozent wie beantragt erlassen werden.

V. Verhältnismäßigkeit und Subsidiarität

Die Beachtung des Verhältnismäßigkeitsgrundsatzes und die Berücksichtigung der Subsidiarität in den Fällen der Funkzellenabfrage und der Zielwahlsuche wurden schwerpunktmäßig in den Expertengesprächen, aber auch in der schriftlichen Befragung analysiert.

1. Schriftliche Befragung

Im Rahmen der schriftlichen Befragung wurden die Staatsanwälte danach gefragt, ob der Verhältnismäßigkeitsgrundsatz ihrer Meinung nach beachtet werde. Die Mehrheit der Befragten (65 Prozent) gab an, dass nie eine Verkehrsdatenabfrage angeordnet werde, wenn es eine mildere gleich geeignete Ermittlungsmaßnahme gebe. 29 Prozent waren der Ansicht, dass dies selten vorkomme und weitere 6 Prozent sprachen davon, dass die Abfrage der Verkehrsdaten in diesen Fällen gelegentlich trotzdem angeordnet werde. Diejenigen, die mit Nie antworteten und eine Begründung abgaben, führten dazu aus, dass die Verkehrsdatenabfrage oft der einzige Ermittlungsansatz sei (27 Prozent dieser Befragten). Zudem wurde angeführt, dass die Maßnahme aufgrund des hohen Aufwands nur beantragt würde, wenn sie auch wirklich notwendig sei (14 Prozent). Nach Ansicht von 12 Prozent sei die Maßnahme nach §§ 100g, 100h StPO ohnehin nur mit einem geringfügigen Eingriff verbunden. Eine mildere Maßnahme in diesem Bereich sei kaum denkbar. 12 Prozent meinen, dass eine Abwägung und Alternativenprüfung immer erfolge. Zu 18 Prozent gaben die Befragten an, dass Ihnen kein Fall bekannt sei, in dem eine mildere Maßnahme verfügbar war und trotzdem §§ 100g, 100h StPO angeordnet wurde. 8 Prozent sind der Ansicht, die Maßnahme werde nur beantragt, wenn sie erforderlich sei. Ein weiterer Teil der Befragten nannte als Begründung, dass die Anwendung der Maßnahme andernfalls rechtswidrig gewesen wäre. Schließlich wurde noch auf Kostengründe hingewiesen.

Diejenigen, die die Häufigkeit als „selten“ einschätzten und dies begründeten, gaben als Begründung an, dass häufig kein anderer Ermittlungsansatz gegeben sei (24 Prozent dieser Befragten). Andere führten aus, dass es vorkommen könne, dass die Verkehrsdatenabfrage in einem solchen Fall angeordnet werde, weil die mildere Maßnahme erst nachträglich erkennbar sei (19 Prozent). 16 Prozent sind der Ansicht, dass eine Abwägung und genaue Prüfung erfolge. 14 Prozent meinten, dass es aus Versehen passieren könne, dass die Verkehrsdatenabfrage durchgeführt werde, obwohl eine mildere Maßnahme vorhanden sei. 11 Prozent gaben an, dass passiere nur, wenn Datenverlust drohe. Weiter wurde angeführt, dass der Grundsatz der Verhältnismäßigkeit berücksichtigt werden müsse, eine mildere Maßnahme viel aufwendiger und weniger erfolgversprechend sei. Einige andere Befragte sind schließlich davon überzeugt, dass der Aufwand der Verkehrsdatenabfrage nur betrieben werde, wenn es auch wirklich erforderlich sei. Die Befragten, die meinten, dass es gelegentlich vorkomme, dass die Verkehrsdatenabfrage angeordnet würde, obwohl eine mildere Maßnahme in Betracht gekommen wäre, führten zur Begründung aus, dass der Zeitdruck dazu führe, den Antrag möglichst schnell zu stellen. Ein intensiver Ermittlungsaufwand hätte wohl zum gleichen Ergebnis geführt, wird weiter angegeben. Weitere Begründung war, dass man erst hinterher wisse, welche Maßnahme erfolgversprechender sei.

2. Aktenanalyse

Im Rahmen der Aktenanalyse konnte die Einhaltung der Subsidiaritätsklauseln und der Verhältnismäßigkeit nicht direkt überprüft werden. Insoweit musste eine Operationalisierung erfolgen. Die Operationalisierung erfolgte durch das Aufgreifen von Ermittlungsalternativen in der Begründung und durch die zeitliche Platzierung der Abfrage im Ermittlungsverfahren. Beides, Begründungen von Anregung, Antrag und Beschluss und die zeitliche Anordnung der Verkehrsdatenabfrage, kann als Indikator für die Berücksichtigung von Subsidiarität und Verhältnismäßigkeit in der Prüfung verwendet werden.

Nur in seltenen Fällen war in den Begründungen von Polizei, Staatsanwaltschaft und Gericht eine detaillierte Auseinandersetzung mit anderen möglichen Ermittlungsmethoden erkennbar; umso seltener waren Ausführungen, warum diese nicht ergriffen werden. Ansonsten deutet die häufige Verwendung der Gesetzesformeln, vor allem des Wortlauts des § 100g II StPO, auf eine eher oberflächliche

Auseinandersetzung mit den Subsidiaritätsklauseln hin (Polizei: 15 Prozent, StA: 28 Prozent, Gericht: 24 Prozent). Die häufige Zitierung des Satzes „Die Erforschung des Sachverhalts wäre auf andere Weise aussichtslos oder wesentlich erschwert“ ohne weitere Ausführungen, warum keine anderen Möglichkeiten alternativ in Betracht kommen, lässt vermuten, dass es sich um eine reine Formalie handelt. Die Klausel wird offenbar aufgenommen, um den Anforderungen des Gesetzeswortlauts formal gerecht zu werden. Letztendlich kann daraus aber nicht eine inhaltliche Auseinandersetzung mit der Subsidiarität abgeleitet werden. Einschränkend ist zu beachten, dass hier wiederum nur die verschriftlichte Auseinandersetzung mit anderen Ermittlungsmöglichkeiten betrachtet werden kann. Über die im Einzelfall tatsächlich angestrengten Erwägungen kann keine Aussage getroffen werden.

Schließlich lässt sich die Berücksichtigung der Verhältnismäßigkeit auch anhand des Einsatzes der Verkehrsdatenabfrage im zeitlichen Ablauf der Ermittlungen abschätzen. Die Verkehrsdatenabfrage ist zumeist eine der ersten Maßnahmen, die zu Beginn des Ermittlungsverfahrens eingesetzt werden und häufig Grund für die erste Einschaltung der Staatsanwaltschaft. Insoweit gibt es Parallelen zum Einsatz der Telekommunikationsüberwachung nach § 100a StPO. Im Übrigen deuten die Einsätze bei Tötungsdelikten und bei Betäubungsmitteldelikten darauf hin, dass es sich hier eben nicht um das „letzte“ Mittel, sondern, umgekehrt, um das „erste“ Mittel handelt. Denn tatsächlich dürfte es bei den Ermittlungen gerade bei Tötungsdelikten zunächst darum gehen, abzuklären, mit welchen Personen das Opfer zuletzt in telefonischem Kontakt stand. Um beurteilen zu können, ob es mildere Maßnahmen gegeben hätte, wäre freilich eine Einzelfallanalyse erforderlich. Insofern lassen sich aus dem Zeitpunkt des Einsatzes der Maßnahme Hinweise, aber keine Nachweise hinsichtlich der Beachtung des Verhältnismäßigkeitsgrundsatzes erbringen. Jedoch deuten die Ergebnisse insgesamt darauf hin, dass gerade die Veränderungen im Kommunikationsverhalten wohl dazu führen, dass sich – deliktsspezifisch – die Ansätze und Ansatzmöglichkeiten in den Ermittlungen so anpassen, dass eben nicht mehr von einer Konkurrenz der Ermittlungsmaßnahmen ausgegangen werden kann. Denn andere gleichermaßen effiziente Möglichkeiten, das Kommunikationsverhalten von Menschen und damit ihre Kontaktpersonen für die Vergangenheit zu ermitteln, gibt es schlicht nicht.

3. Experteninterviews

Zum Thema der Subsidiarität wurden die Befragten um Stellungnahme zu kritischen Anmerkungen mehrerer Telekommunikationsunternehmen gebeten. Deshalb sollen die Ergebnisse der Befragung der Diensteanbieter an dieser Stelle vorangestellt werden.

a) Telekommunikationsunternehmen

(1) Verhältnismäßigkeit

Die Mitarbeiter der Hälfte der befragten Unternehmen sind der Meinung, dass die Maßnahmen teilweise nicht verhältnismäßig seien. So seien die Anlassdelikte oft nur Bagatellfälle (z. B. Fundunterschlagung oder Diebstahl von Endgeräten). Weiterhin würden „Ermittlungen ins Blaue hinein“ erfolgen. Abfragen im Zusammenhang mit Einbruchsdiebstählen seien alleine mit der Begründung gestartet worden, dass „erfahrungsgemäß bei diesen Straftaten telefoniert wird“. Aufgrund solcher pauschalen Hinweise würden dann alle großen Anbieter zur Funkzellenabfrage verpflichtet. Ganze Bahnhöfe würden über einen längeren Zeitraum abgefragt. Wenn die Behörden die Kosten selbst tragen müssten, würden deutlich weniger Anfragen gestellt werden, meinte einer der Befragten. Die Anordnung der Maßnahme nach §§ 100g, 100h StPO sei früher eher ultima ratio gewesen, jetzt sei es der erste Ansatz, wird weiter ausgeführt. Innerhalb der Maßnahme sei die Anordnung oft nicht begrenzt genug, d. h. das Datenvolumen sei zu groß. Es würden so viele Daten wie möglich abgefragt. Dies sei jedoch ein erheblicher Aufwand für die Anbieter und vor allem auch für die Polizei. Diese Datenmengen könnten nicht effektiv bearbeitet werden, so ein Befragter, zum Beispiel bei der Datenabfrage zu bestimmten Bahnstrecken. Es sei daher wünschenswert, wenn der Beschluss bzw. die Anfrage sich auf weniger Daten beschränken würde und konkreter gefasst wäre. Das Verhältnis zwischen Grundrechtseingriff und verfolgter Straftat stimme nicht, wird weiter erläutert. Die Zweck-Mittel-Relation zwischen dem Fernmeldegeheimnis der Kunden und der Berufsfreiheit der Telekommunikationsanbieter und dem Strafverfolgungsinteresse sei unstimmig. Artikel 10 GG habe seinen Stellenwert eingebüßt. Gerade die Möglichkeit der Anordnung bei mittels Endeinrichtung begangener Straftat eröffne Tür und Tor. Einfache Beleidigungen sollten aber nicht ausreichen. Bei der Zielwahlsuche würden Millionen Menschen betroffen. Alle Kunden würden einmal am Tag daraufhin gerastert, wen sie angerufen haben. Sehr viele Personen (Polizei, Staatsanwälte, Richter, Telekommunikationsanbieter) seien mit den Anordnungen beschäftigt und das teilweise wegen Schadenhöhen von unter 10 Euro. Die Masse der Fälle betreffe nach den Erfahrungen der Telekommunikationsunternehmen Bagatellbeträge und -delikte, nicht die Schwerstkriminalität. Einige der Befragten möchten keine Stellungnahme abgeben, weil ihnen die Hintergründe fehlen würden. Außerdem seien sie zur Auskunft verpflichtet. In bestimmten Fällen hätten sie Zweifel bei der Verhältnismäßigkeit, so beispielsweise bei Autodiebstählen und Diebstählen von Mobiltelefonen. Vor allem bei Handydiebstählen sei die Verhältnismäßigkeit problematisch, da der jetzige Nutzer aller Voraussicht nach nicht derjenige sei, der das Mobiltelefon gestohlen habe. Aber es sei nicht ihre Aufgabe, dies zu beurteilen.

(2) Häufigkeit der Anfragen

Ob die Maßnahmen ihrer Meinung nach zu häufig angeordnet werden, beantworteten die befragten Mitarbeiter der Telekommunikationsunternehmen unterschiedlich. Ein Befragter gibt an, dass sie dies nicht beurteilen könnten. Sie hätten kein Prüfungsrecht und würden die Hintergründe nicht kennen. Mit Blick auf die Massenhaftigkeit der Anfragen könne man aber davon ausgehen, dass die Maßnahmen zu häufig seien, meint ein anderer Befragter. Ein anderer Befragter gibt an, dass eine generelle Steigerung der Anordnungen zu verzeichnen sei. Die Mitarbei-

ter von zwei Anbietern sind der Ansicht, dass die Maßnahmen zu häufig eingesetzt würden. Die Verkehrsdatenabfrage sei eine Standardmaßnahme geworden, die routinemäßig eingesetzt werde. Es erfolge keine ausreichende Prüfung. Schon bei simplen Beleidigungen oder Fundunterschlagungen gebe es Anordnungen nach §§ 100g, 100h StPO. Auch die IMEI-Abfragen wegen gestohlener Mobiltelefone beträfen einen erheblichen Teil der Anordnungen. Terrorismus und die Bekämpfung der Kinderpornographie, die stets als Begründung für die Maßnahmen herangezogen würden, seien in der Praxis eher selten. Stattdessen werde die Abfrage wegen Betäubungsmitteln im Bagatellbereich angeordnet.

b) Polizeibeamte

(1) Verhältnismäßigkeit

Den befragten Polizeibeamten wurden mit diesen Aussagen der Telekommunikationsanbieter konfrontiert, teilen die Bedenken aber in der Mehrzahl nicht. Es herrsche ein angemessenes Verhältnis zwischen Tatvorwurf und Mittel. Die Verhältnismäßigkeit werde geprüft und schon dadurch, dass drei Stellen an dem Vorgang beteiligt sind (Polizei, StA und Gericht) gewahrt. Es komme immer auf den Einzelfall an – gerade in Bezug auf die Verhältnismäßigkeit. Bei Schwerstkriminalität (organisierte Kriminalität, Betäubungsmitteldelikte) sei die Verhältnismäßigkeit immer gewahrt. Bei mittlerer oder einfacher Kriminalität würde der Aufwand, umfassendere Verkehrsdaten auszuwerten, nicht betrieben. Der Richtervorbehalt garantiere die Prüfung durch eine rechtlich unabhängige Instanz und Richter würden keine Gefälligkeitsbeschlüsse erlassen. Die Daten würden soviel Auswertungskapazität verlangen, dass allein aus verfahrensökonomischen Gründen genau überlegt werde, ob die Maßnahme beantragt werden solle. Die Polizei beantrage die Maßnahme nur, wenn sie Erfolg versprechend sei. Oft sei es die letzte Möglichkeit, um den Täter zu ermitteln. Einer der Befragten aus einer Abteilung für Computerkriminalität gibt an, dass die Polizei in ihrem Bereich ohne Verkehrsdaten gar nicht in der Lage sei, weitere Ermittlungen aufzunehmen. Prinzipiell wird kritisiert, dass die Anbieter nicht in der Lage seien, diesen Aspekt zu würdigen, da sie die Aktenlage nicht kennen würden. Teilweise gaben die Befragten an, dass den Providern die Beschlüsse ohne Gründe zugestellt würden und dass sie deshalb die Verhältnismäßigkeit nicht beurteilen könnten. Einer der Befragten meint hingegen, die Einschätzung sei im Großen und Ganzen zutreffend. „Im Eifer des Gefechts käme es schon mal vor, dass die eine oder andere Abfrage nicht sinnvoll war“, räumt er ein. Das erfolge aber nicht bewusst. Ein weiterer Polizist gibt an, dass dies im Einzelfall möglich sei. Polizei und Staatsanwaltschaft hätten ein Strafverfolgungsinteresse und richteten den Blick auf den Erfolg. Das Gericht könne gar nicht vollumfänglich prüfen.

(2) Berücksichtigung der Subsidiaritätsgrundsätze

Die Frage nach der hinreichenden Berücksichtigung der Subsidiaritätsgrundsätze bei der Funkzellenabfrage und der Zielwahlsuche bejahten die meisten befragten Polizeibeamten. Die Maßnahmen seien sehr wohl ultima ratio. Begründet wurde dies mit der Flut von Massendaten, die man vermeiden wolle. Der Aufwand für die Auswertung sei für die bearbeitende Dienststelle sehr hoch. Wenn es andere Möglichkeiten gebe, würden diese auch ergriffen werden. Wenn es aber dringend notwendig sei, dann müssten Ressourcen (Personal) geschaffen werden. Am Anfang der Ermittlungen seien andere Maßnahmen meist noch aussichtslos oder wesentlich erschwert. Die Verkehrsdatenabfrage, insbesondere die Zielwahlsuche, sei oft das einzige Mittel, z. B. bei Bedrohung. Außerdem stehe stets die Gefahr der Löschung im Raum. Man leite diese Maßnahmen deshalb oft bereits parallel zu anderen ein. Ob sich jemand an einem bestimmten Ort aufgehalten und telefoniert habe, könne man eben nur mit diesem Mittel überprüfen. Die Abfrage werde zwar als Standardmaßnahme eingesetzt. Gleichwohl werde aber geprüft, ob die Ergebnisse auch mit anderen Ermittlungsmaßnahmen erreicht werden könnten. Die Richter würden genau darauf achten, ob die Voraussetzungen der Maßnahme vorliegen. Sie würden insbesondere auch prüfen, ob überhaupt telefoniert worden sei. Die Prüfung der Subsidiarität sei notwendig, da eine hohe Anzahl Nichtbeschuldigter überprüft werde. Vier der Befragten gaben an, dass diese Maßnahmen wegen häufiger Durchführung von Telekommunikationsüberwachungen bei ihnen relativ selten vorkämen (drei Befragte aus Betäubungsmittel-Abteilungen und einer aus einem Telekommunikationsüberwachungskommissariat). Diese Überwachungsmaßnahmen würden z. B. die Standortdaten mit sich bringen. Nur um neue Ermittlungsansätze zu bekommen, würden Funkzellenabfragen durchgeführt (Prüfung auf Überschneidung in verschiedenen Funkzellen). Teilweise schließen die Befragten nicht aus, dass es andere Mittel gegeben hätte. In dem Stadium sei es aber noch nicht erkennbar gewesen, ob diese anderen Ermittlungsmaßnahmen erfolgreich gewesen wären. Mitunter wird zugegeben, dass die Ermittler eine Maßnahme immer durchsetzen würden, wenn sie es wollen. Sie müssten es nur entsprechend begründen. Die Subsidiaritätsgrundsätze würden wenig Wirkung entfalten.

(3) Gründe für die Zunahme der Anordnungen

Die Zunahme der Anordnungen nach §§ 100g, 100h StPO wurde von den Befragten in unterschiedlicher Weise erklärt. Die Telekommunikation an sich habe zugenommen und habe sich verändert, gaben die meisten der Befragten an. Jeder habe heutzutage mindestens ein Mobil- und ein stationäres Telefon. Die Zunahme beruhe also auf der Entwicklung im Kommunikationsbereich. Der Trend gehe zu mehreren Mobiltelefonen (zwei bis drei). Die aktuelle Zahl von 82 Millionen Mobilfunkteilnehmern belege dies. Früher habe ein Täter ein Mobiltelefon und ein Festnetztelefon gehabt. Heute habe eine Person einen ISDN-Anschluss mit vier bis sechs Nummern, einen Internetanschluss, worüber er VoIP durchführe, E-Mails schreibe etc. Einzelne Täter hätten heute bis zu 20 Rufnummern. Es herrsche eine stetig fortschreitende Verbreitung von Telekommunikationsmöglichkeiten und

Endgeräten. Es sei kaum noch eine Straftat ohne Telekommunikation vor, während oder nach der Tat denkbar. Täter nutzen zur Verschleierung der Straftaten bewusst mehrere Rufnummern oder IP-Adressen. Der ständige Kartenwechsel treibe die Statistik in die Höhe, gab die Hälfte der befragten Polizeibeamten an: fünf Kartenwechsel erfordern eben fünf Beschlüsse. Die Täter wechselten häufig die Mobiltelefone und Karten. Bei mehreren Tätern käme es mitunter vor, dass diese 60 Anschlüsse unterhalten. Von einem anderen Befragten wurde angeben, dass die Anschlüsse im Tagestakt gewechselt würden. Die Möglichkeit, Kennungen zu wechseln, sei sehr leicht. Man müsse sich den Tätern daher anpassen und für jede neue Kennung einen neuen Beschluss beantragen, obwohl es sich um ein und dasselbe Individuum handle. Die Vertragsbeziehungen seien durch Prepaid-Karten und Internet unklar. Es gebe nicht mehr Zielpersonen, sondern mehr Anschlüsse und Anschlusswechsel als früher.

Zudem gebe es heutzutage viel mehr technische Möglichkeiten und die Polizei könne die Möglichkeiten der Telekommunikationsanbieter-Auswertung aufgrund von Schulungen heute auch viel besser einsetzen. Die Maßnahme habe schon öfter bei herausragenden Delikten zum Erfolg geführt, so dass dann auch bei anderen Delikten darauf zurückgegriffen werde. Weiterer Grund für die Zunahme sei, dass mittlerweile auch IMEI-Abfragen möglich seien. Der Raub von Mobiltelefonen sei damit besser aufklärbar. Sobald der Täter das Mobiltelefon benutze, sei er über die IMEI zu fassen.

c) Staatsanwälte

(1) Verhältnismäßigkeit

Auch die Staatsanwälte teilten die kritische Bewertung einiger Telekommunikationsanbieter in ihrer großen Mehrheit nicht. Schon aufgrund des hohen Arbeitsaufwandes (Beantragung, Auswertung der Daten bei der Polizei), werde sie nur beantragt, wenn keine andere Ermittlungsmaßnahme in Betracht komme. Die Voraussetzungen würden sowohl seitens der Staatsanwaltschaft als auch des Gerichts geprüft. Die Wahrung der Verhältnismäßigkeit werde gründlich geprüft und konsequent eingehalten. Die Maßnahme werde nicht wegen Bagatellen durchgeführt. Wenn andere Maßnahmen parallel liefen, würde erörtert werden, warum jetzt auch noch diese Maßnahme erforderlich ist. Ein Befragter räumt ein, dass die Verhältnismäßigkeit inhaltlich beachtet würde, es mitunter aber an der Begründung mangele. Ein Befragter aus einer Computerabteilung gibt an, dass es sich in der Regel um Maßnahmen handelt, die unbekannte Täter zum Ziel haben. Dabei könne man nicht vorab beurteilen, ob es um einen professionellen Hacker oder einen Jungenstreich gehe. Das stelle sich erst dann heraus, wenn der Täter ermittelt sei. Die Fälle, in denen die Maßnahme letztendlich nicht beantragt würde, würden die Provider gar nicht wahrnehmen. Einige Staatsanwälte wenden ein, dass die Anbieter nichts über die Einzelheiten des Verfahrens wüssten. Sie würden die Akten nicht kennen und könnten überhaupt nicht beurteilen, welche alternativen Möglichkeiten bestehen. Entweder erhalten sie die Gründe zum Beschluss überhaupt nicht oder nur eine Begründung ohne Einzelheiten. Eine Einschätzung der Verhältnismäßigkeit sei also gar nicht möglich. Teilweise sind die Befragten der Ansicht, dass die Provider die Verhältnismäßigkeit nicht zu beurteilen hätten. Das entscheide die Justiz.

(2) Berücksichtigung der Subsidiaritätsgrundsätze

Die Subsidiaritätsgrundsätze würden bei der Funkzellenabfrage und der Zielwahlsuche besonders berücksichtigt, gibt die Hälfte der Befragten an. Diese Maßnahmen würden einen noch höheren Aufwand bedeuten und daher (allein aus praktischen Gründen) nur durchgeführt, wenn tatsächlich keine anderen Ermittlungsmöglichkeiten vorhanden seien. Problematisch seien aber die zu kurzen Speicherungszeiten. Wenn die Maßnahme nicht zu Beginn durchgeführt würde, könnten sie sie gar nicht mehr nutzen. Die Subsidiaritätsgrundsätze würden in sinnvoller Weise den Einsatz der Maßnahmen in Fällen verhindern, in denen es andere Ermittlungsmöglichkeiten gebe. Eine große Bedeutung kommt der Begründung zu. Es gebe oft andere Maßnahmen, die aber weniger Erfolg versprechend sind. Dann müsse man die Maßnahme entsprechend begründen. Bei der Zielwahlsuche und der Funkzellenabfrage müsse man zudem abwägen, da viele Unbekannte davon betroffen sind. Ein Befragter meint, die Funkzellenabfrage werde nur als letzte Möglichkeit verwendet. Bei einem Bankraub sei es aber wichtig, im Umfeld der Bank eine Funkzellenabfrage durchzuführen, um überhaupt Täter ermitteln zu können. Wenn man schon Hinweise auf die Täter habe, sei die Maßnahme wichtig, um Mittäter und das Umfeld der Verdächtigen zu ermitteln. In solchen Fällen sei die Maßnahme unabdingbar. Bei den Subsidiaritätsgrundsätzen handle sich um eine „Gummiformulierung“, meint ein Befragter. „Wesentlich erschwert“ seien die Ermittlungen eigentlich immer. Deswegen führe man die Maßnahmen ja durch. Die Voraussetzung der Aussichtslosigkeit der Ermittlungen sei dagegen schwieriger zu begründen.

(3) Gründe für die Zunahme der Anordnungen

Die Zunahme der Anordnungen nach §§ 100g, 100h StPO erklären sich auch die befragten Staatsanwälte u. a. mit dem zunehmenden Einsatz von Telefonen bei den Tätern. Es herrsche eine veränderte Form der Kriminalität und Benutzung der neuen Medien. Die Kriminalität, in der Telekommunikation eine Rolle spielt, nehme zu. Es gebe kaum eine Straftat, bei der Telefone keine Rolle spielen und damit auch die entsprechenden Verbindungen. Die Zahl der Anschlüsse steige stetig an und Mobiltelefonen käme in der heutigen Gesellschaft eine grundlegende Bedeutung zu. Ein weiterer Faktor für die Zunahme der Anordnungen sei die Zunahme der Delikte mittels Internet, meint ein Befragter aus der Computerkriminalitätabteilung. Das Täterverhalten werde immer trickreicher, immer konspirativer. Der häufige Wechsel der Mobilfunkanschlüsse sei hierfür ein Beleg. Es würden immer wieder neue Prepaidkarten und neue Rufnummern organisiert.

Dann bedürfe es auch immer wieder neuer Beschlüsse. Zudem habe die Methode Erfolg gebracht, was zu häufigeren Beschlüssen führe. Herkömmliche Methoden wie Observationen würden nicht ausreichen. Ohne §§ 100g, 100h StPO wären die Ermittlungen wesentlich erschwert. Die Polizei versuche, alle Ermittlungsmöglichkeiten auszuschöpfen. Die technischen Möglichkeiten, die es gebe, würden auch genutzt. Außerdem gibt ein Befragter zu Bedenken, dass im Gegenzug eine Abnahme der Postbeschlagnahme zu verzeichnen sei. Statt Briefen gebe es heute eben SMS und Telefone.

d) Richter

(1) Verhältnismäßigkeit

Die Bewertung einiger Diensteanbieter, was die Verhältnismäßigkeit der Maßnahmen angeht, teilt fast keiner der befragten Richter. Strafverfolgung bedeute Rechtsgüterschutz. Bei geringfügigen Delikten könnten Maßnahmen in der Tat unverhältnismäßig werden. Die Aufklärung von Straftaten sei anders oft nicht möglich. Die Häufigkeit der Maßnahmen gehe mit den technischen Möglichkeiten und dem Verhalten der Beschuldigten (ständiger SIM-Karten-Wechsel) einher. Im Fokus stünden oft Personen in Altersbereichen, die viele Festnetzanschlüsse und viele Mobiltelefone hätten (Prepaidkarten; eigene Anschlüsse, Anschlüsse der Eltern/Freunde). Auch in der übrigen Gesellschaft werde wesentlich mehr Kommunikation über Mobiltelefone abgewickelt als früher. Ein Befragter ist der Ansicht, dass die Polizei teilweise übertreibe, da die Abfrage der Daten für sie relativ einfach sei. So würden teilweise auch bei Belästigungen und einfachen Diebstählen Anträge nach §§ 100g, 100h StPO gestellt. Für den Zugriff auf Verkehrsdaten bedürfe es aber einer erheblichen Straftat. Diese Anträge würden vom Gericht abgelehnt. Die Telekommunikationsanbieter hätten die Verhältnismäßigkeit überhaupt nicht zu prüfen, meinen vier der Richter. Dies sei Aufgabe des Gerichts. Ein Befragter ist der Ansicht, dass sie dies auch gar nicht prüfen könnten. Bei ihnen würden die Beschlüsse an die Anbieter ohne Gründe verschickt.

(2) Berücksichtigung der Subsidiaritätsgrundsätze

Zwei der befragten Richter sind der Ansicht, dass die Subsidiaritätsgrundsätze bei der Funkzellenabfrage und der Zielwahlsuche hinreichend berücksichtigt werden. Die Staatsanwaltschaft würde viele Anregungen ablehnen, durchaus auch in Fällen, in denen die Maßnahme möglich wäre. Gerade bei organisierter Kriminalität und Kapitalverbrechen komme man an den Kreis möglicher Zeugen aber sonst nicht heran. Auch bei dem Raub von Mobiltelefonen bleibe nur die Möglichkeit, den Standort des Telefons zu ermitteln. Ein Befragter gibt an, dass die Subsidiarität zwar geprüft werde, aber in der Praxis kaum eine Rolle spiele. Die Polizei sei auf die Daten angewiesen. Die Subsidiaritätsgrundsätze würden von der Polizei nicht immer hinreichend berücksichtigt, gibt einer der befragten Richter an. Er schätzt die Maßnahme teilweise als eine Suche nach Zufallsfunden ein. Die Beschlüsse würden teilweise abgelehnt, daraufhin ggf. Beschwerde eingelegt und das Beschwerdegericht entscheide unterschiedlich. Nach der Meinung von weiteren Befragten werden die Subsidiaritätsgrundsätze generell nicht besonders beachtet. Funkzellenabfragen würden sehr ausufernd in Bezug auf Ort und Zeit beantragt. Er werde dann versucht, die Anzahl der zu überwachenden Funkzellen auf möglichst wenige und die Maßnahme auf einen engen Zeitraum zu reduzieren. Ein anderer Richter findet, dass die Subsidiaritätsgrundsätze entfallen könnten. Es würde dann eine normale Verhältnismäßigkeitsprüfung erfolgen und das sei ausreichend.

(3) Gründe für die Zunahme der Anordnungen

Auch die Richterschaft sieht verschiedene Gründe für die Zunahme der Anordnungen nach §§ 100g, 100h StPO. Die Vielzahl von Festnetzanschlüssen und Handys, die Zunahme von Telefonaten im Allgemeinen und die vermehrte Nutzung von Handys im Besonderen. Letztere würden bei Straftaten eine sehr große Bedeutung einnehmen. Es würden Absprachen damit erfolgen vor, während und nach der Tat. Dies sei vor allem beim sog. Enkelbetrug und auch bei Betäubungsmittelsachen zu bemerken. Die Häufigkeit der Maßnahmen gehe auch mit dem Verhalten der Beschuldigten (ständiger SIM-Karten- und Mobiltelefonwechsel) einher. Die Täter würden die Ermittlungsmaßnahme mittlerweile einkalkulieren und ihre Kontakte regelmäßig ändern. So werde beim Drogenhandel 6- bis 7-mal am Tag das Mobiltelefon gewechselt. Für jedes Mobiltelefon werde aber ein neuer Beschluss benötigt. Pro Anbieter ergehe ein Beschluss mit neuem Aktenzeichen, erläutert ein Richter aus Nordrhein-Westfalen. Es würden dann teilweise bei allen Anbietern Daten abgefragt, weil unklar sei, bei welchem Anbieter der Anschluss betrieben wird. Ein anderer Richter berichtet von Verfahren mit bis zu 30 Beschlüssen. An sich gebe es also gar nicht so viele Fälle mit Telefonüberwachung und Verkehrsdatenabfrage, wohl aber Verfahren mit vielen Beschlüssen. Speziell in Mecklenburg-Vorpommern und Nordrhein-Westfalen ist offensichtlich eine Steigerung bei Betäubungsmitteldelikten festzustellen. Ein Drittel aller Fälle dort seien Betäubungsmittelsachen, berichtet ein Richter aus Nordrhein-Westfalen. Auch Internetstrafsachen würden zunehmen. So verzeichnet Berlin 400 Anträge pro Monat wegen des Herunterladens von CDs aus dem Internet. Schließlich wird wiederum auf die Verfügbarkeit der technischen Voraussetzungen verwiesen, welche die Polizei bzw. die Ermittlungsbehörden dann auch nutzten. Es entstehe der Eindruck, dass die Polizei es als Kunstfehler ansehe, wenn die technischen Möglichkeiten nicht genutzt werden. Die Polizei werde bzgl. der Ermittlungsmaßnahmen geschult und könne ziemlich viel steuern, meint ein anderer Richter. Weiter wurde angegeben, dass die alte Vorschrift nicht so bekannt gewesen sei. Jetzt sei die Maßnahme konkreter geregelt und daher auch verbreiteter. Ein Befragter sagte, dass er die Sorge, dass Deutschland zu einem Abhörstaat werde, wenn die Anordnungen zunehmen, nicht teilen könne.

e) Verteidiger

(1) Verhältnismäßigkeit

Fast alle befragten Verteidiger schätzen die Äußerung einiger Telekommunikationsanbieter, dass die Polizei- und Justizbehörden teilweise den Verhältnismäßigkeitsgrundsatz nicht berücksichtigen, als richtig ein. Die Behörden würden einen Vorwand suchen, um die Daten zu erlangen, so dass beispielsweise eine bandenmäßige Begehung vorgeschoben würde, um die Maßnahme anordnen zu können. Des Weiteren unterstellen die befragten Verteidiger, dass der Verhältnismäßigkeitsgrundsatz – wie bei allen Zwangsmaßnahmen – großzügig gehandhabt würde. In vielen Verfahren hätte es weniger einschneidende Möglichkeiten gegeben. Es entstehe der Eindruck, dass es einen bestimmten Katalog an durchzuführenden Maßnahmen gebe, der abgehakt wird. Das wird auch daraus geschlossen, dass die Behörden Vordrucke verwenden, die nur noch ausgefüllt werden müssen. Eine inhaltliche Überprüfung finde überhaupt nicht statt, was aber auch daran liege, dass weder Zeit noch Mittel vorhanden seien, um sorgfältig zu prüfen. Die Verhältnismäßigkeit werde in der Begründung mit dem Satz „Die Verhältnismäßigkeit ist gewahrt“ abgehandelt. Je mehr zulässig ist, desto weniger würde darauf geachtet, eine bestimmte Reihenfolge bei den durchzuführenden Maßnahmen einzuhalten. Es werde nicht gewartet, bis alle anderen Wege ausgeschöpft sind, sondern es werde der schnellen, effektiven Aufklärung der Vorrang eingeräumt.

(2) Berücksichtigung der Subsidiaritätsgrundsätze

Alle befragten Verteidiger verneinten die Frage, ob Ihrer Meinung nach die gesetzlich festgelegten Subsidiaritätsgrundsätze bei der Funkzellenabfrage und der Zielwahlsuche hinreichend berücksichtigt würden. Dem Grundsatz der schnellen, effektiven Strafverfolgung werde der Vorrang eingeräumt. Die Maßnahme werde unmittelbar und sofort angewendet. Für die Begründung werde lediglich der Wortlaut des Gesetzes abgeschrieben.

(3) Gründe für die Zunahme der Anordnungen

Die Zunahme der §§ 100gh-Maßnahmen erklären sich die befragten Verteidiger unterschiedlich. Zum einen wird angeführt, dass die Verdächtigen früher nur telefoniert hätten, heute dagegen finde die Kontaktaufnahme auch über E-Mail statt, ggf. auch über Provider im Ausland. Die Polizei und Justiz verfüge über neue Möglichkeiten und könne die Straftaten unmittelbar mitverfolgen. Es finde sozusagen schon eine „präventive Überwachung“ statt. Zunächst würden so viele Daten gesammelt wie möglich, um erst dann zu prüfen, was damit angefangen werden könne. Weiter wurde geäußert, dass es sich um eine sehr bequeme Möglichkeit der Strafverfolgungsbehörden handle, um mit den Ermittlungen zu *beginnen*. Als Argument werde gerne der 11.September 2001 angeführt. Einer der Befragten ist der Ansicht, dass sich die Gründe für die Zunahme der §§ 100a, 100b-Maßnahmen auf §§ 100g, 100h-Maßnahmen übertragen ließen. Außerdem sei die Abfrage der Verkehrsdaten ein guter Ansatzpunkt, um herauszufinden, mit wem der Beschuldigte telefoniert habe, um anschließend eine Telekommunikationsüberwachung anzuordnen. Erklärt wurde die Zunahme ferner damit, dass überhaupt erst von dem Instrument Notiz genommen worden sei, nachdem die Maßnahme in die Strafprozessordnung integriert wurde. § 12 FAG dagegen sei von den Staatsanwälten meist gar nicht beachtet worden. Außerdem sei ein Zusammenhang mit dem Telekommunikationsverhalten der Bevölkerung gegeben, da immer mehr telefoniert würde. Schließlich koste es die Behörden weder Zeit noch Geld, da die Anbieter die Maßnahmen durchzuführen hätten.

f) Datenschützer

(1) Verhältnismäßigkeit und Subsidiarität

Alle befragten Datenschützer halten die teilweise Unverhältnismäßigkeit der Maßnahmen zumindest für plausibel. Einer der Befragten schließt dies aus selbst eingesehenen Vorgängen. Aus diesen sei ersichtlich, dass nur ein vager Verdacht vorhanden gewesen sei, dass aber trotzdem noch die §§ 100g, 100h-Maßnahmen durchgeführt worden seien. Es werde wahrscheinlich doch ziemlich schnell zur Maßnahme nach §§ 100g, 100h StPO gegriffen und nicht erst alle anderen Mittel ausgeschöpft. Die Maßnahme sei zu einer polizeilichen Standardmaßnahme geworden. Im Rahmen der Verhältnismäßigkeitsprüfung müssten die Schwere der Straftat und die Anzahl der auch unbeteiligten betroffenen Dritten gegeneinander abgewogen werden. Das werde wohl häufig nicht eingehalten. Alle Befragten gaben jedoch an, dass sie nur eine eingeschränkte Prüfungsmöglichkeit haben und die Handhabung in der Praxis nicht genau kennen.

(2) Eingriffsintensität der Maßnahme

Die Eingriffsintensität der Maßnahmen im Verhältnis zu anderen Ermittlungsmaßnahmen wird aus datenschutzrechtlicher Sicht von allen Befragten als hoch bewertet. Gegenüber offenen Ermittlungsmaßnahmen sei ohnehin eine gesteigerte Eingriffsintensität gegeben. Zudem sei die Intensität des Eingriffs in Grundrechte – auch im Vergleich zu anderen verdeckten Methoden – relativ hoch, da auch viele Unverdächtige betroffen seien. Natürlich gebe es aber andere Maßnahmen, die noch stärker in die Grundrechte eingreifen. Im Verhältnis zu § 100a StPO kratze die Telekommunikationsüberwachung zwar häufiger am Kernbereich privater Lebensgestaltung, da der Inhalt der Telekommunikation in Erfahrung gebracht wird. Über § 100g, 100h StPO erfahre man zwar keine Inhalte, aber Kontakte zu Ärzten, Psychiatern, Aids-Krankenstellen usw. Dies seien auch sehr sensible Daten. Problematisch wäre zudem, dass es – im Gegensatz zu § 100a StPO – Raum für Interpretationen und Schlussfolgerungen gebe. Auch daraus würde sich die erhebliche Eingriffsintensität ergeben. Weiter wurde ausgeführt, dass ein Eingriff ins Recht auf informationelle Selbstbestimmung und ins Fernmeldegeheimnis durch die Maßnahmen erfolge. Auch wenn keine Inhaltsdaten abgefragt würden, könne man feststellen, wer mit wem über welches Medium

kommuniziert habe. Anhand dessen könne man Neigungen und Interessen nachvollziehen, beispielsweise über aufgerufenen Internetseiten. Damit könnten Verhaltensprofile erstellt werden, die u.U. die Aussagekraft von Inhaltsdaten übertreffen könnten. Die Verkehrsdaten würden außerdem das soziale Netz, in dem sich der Betroffene bewegt, widerspiegeln. Das sei von der gleichen Eingriffsintensität wie ein Bewegungsprofil, welches über das soziale Umfeld ggf. mehr aussagt als die Information, wo sich der Betroffene aufgehalten hat. Angeführt wurde auch, dass die Maßnahmen der §§ 100g, 100h StPO häufig der Vorbereitung der anderen Maßnahmen, insbesondere der Vorbereitung der Telekommunikationsüberwachung, dienen. Sie ähnle zumindest in ihren Auswirkungen der Rasterfahndung, da Unverdächtige davon erfasst würden. Auch durch den betroffenen Personenkreis ergebe sich eine hohe Eingriffsintensität. Ein Datenschützer sprach zudem das Gewicht der Kommunikation für das Gemeinwesen an. Es entstehe ein Überwachtheitsgefühl. Man müsse sich überlegen, mit wem man telefoniert. Auch das Bundesverfassungsgericht habe festgestellt, dass die Auswirkungen auf die Ausübung der Grundrechte berücksichtigt werden müsste. Die Verkehrsdatenabfrage und auch die Vorratsdatenspeicherung würden sich jedoch stark auf die Ausübung auswirken.

(3) Gründe für die Zunahme der Anordnungen

Für die Zunahme der Anordnungen nach §§ 100g, 100h StPO wurden unterschiedliche Erklärungsansätze herangezogen. Zum einen wurde angeführt, dass bestimmte Dinge vom Büro aus ermittelt werden sollen und Observationen o. ä. aufwendiger seien. Die Verkehrsdatenabfrage sei für die Strafverfolgungsbehörden kostengünstig und bedeute wenig Aufwand. Letzteren hätten dann die Provider. Es wurde weiter geäußert, dass von offizieller Seite sicher kommen werde, dass die Zunahme des Mobilfunkverkehrs der Grund für die Zunahme der Anordnungen sei. Es seien mehr Anschlüsse pro Person zu verzeichnen. Außerdem finde in bestimmten Milieus ein ständiger Kartentausch statt, so dass bzgl. eines Betroffenen mehrere Anordnungen erforderlich seien. Die Statistiken würden für diese Gründe sprechen. Aber §§ 100g, 100h StPO sei eine sehr praktikable Maßnahme. Daher wird vermutet, dass sie auch gern angeordnet werde. Zudem gehe man davon aus, dass potentielle Täter miteinander telefonieren auch während eine Straftat begangen wird. Die Anordnungen würden oftmals der Verdachtsschöpfung dienen.

4. Zusammenfassung der Ergebnisse

Die Verhältnismäßigkeit der Maßnahmen und die Beachtung der Subsidiarität ließen sich größtenteils nur anhand der Befragungen untersuchen. Die Aktenanalyse konnte nur Hinweise durch die Begründungen von Anregung, Antrag und Beschluss und durch den Zeitpunkt des Einsatzes der Verkehrsdatenabfrage im Verhältnis zu anderen Ermittlungsmaßnahmen geben. Bei den Begründungen durch Polizei, Staatsanwaltschaft und Gericht fällt auf, dass relativ häufig die Formulierung der Subsidiaritätsklauseln in § 100g II StPO und des § 100h I Satz 2 StPO wörtlich in die Begründung aufgenommen werden (Polizei 18 Prozent, Staatsanwaltschaft 28 Prozent und Gericht 24 Prozent der Fälle). Die Übernahme der Formulierung, dass die „Ermittlung des Sachverhalts sonst aussichtslos oder wesentlich erschwert wäre“ spricht aber nicht dafür, dass hier eine intensive Auseinandersetzung mit der Subsidiarität stattgefunden hat. Zwar lässt sich die inhaltliche Beschäftigung mit diesem Aspekt den Begründungen nicht entnehmen. Es ist jedoch ein Anzeichen dafür, dass der Satz aufgenommen wird, damit der Beschluss formal korrekt ist, und nicht dafür, dass der Inhalt auch tatsächlich zutrifft. Weiteres Kriterium zur Beurteilung der Einhaltung der Verhältnismäßigkeit ist der Einsatz der Maßnahme im Ablauf des Ermittlungsverfahrens. Die Verkehrsdatenabfrage wird nach den Ergebnissen der Aktenanalyse überwiegend zu Beginn des Ermittlungsverfahrens eingesetzt. Dies wird im Folgenden noch differenzierter dargestellt.

Aus den Interviews mit den Experten lässt sich entnehmen, dass einige der befragten Telekommunikationsanbieter, die Verteidiger und die Datenschützer der Ansicht sind, dass die Polizei- und Justizbehörden den Verhältnismäßigkeitsgrundsatz nicht hinreichend berücksichtigen. Erstere führen dazu vor allem die Unverhältnismäßigkeit des Eingriffs in das Fernmeldegeheimnis in Relation zur verfolgten Tat an. Die den Beschlüssen zugrunde liegenden Delikte seien überwiegend nicht dem Bereich der Schwerstkriminalität zuzuordnen, sondern es handle sich um geringfügigere Delikte wie Diebstahl von Mobiltelefonen und kleinere Betäubungsmitteldelikte. Zudem seien die Beschlüsse zu weit gefasst und oftmals nicht hinreichend konkretisiert. Auch die Masse der Datenabfragen wird als Beleg dafür interpretiert, dass die Verhältnismäßigkeit nicht immer gewahrt sei. Ferner sind die befragten Verteidiger der Ansicht, dass der schnellen, effektiven Aufklärung der Straftat der Vorrang vor dem Verhältnismäßigkeitsgrundsatz eingeräumt werde. Die Maßnahme sei oftmals der erste Ansatzpunkt, mit dem die Ermittlungen beginnen. Polizeibeamte, Staatsanwälte und Richter dagegen sind größtenteils der Ansicht, dass die Verhältnismäßigkeit und die Subsidiaritätsgrundsätze beachtet werden. Allein der mit der Verkehrsdatenabfrage verbundene Aufwand der Datenauswertung führe dazu, dass die Maßnahme nur beantragt werde, wenn sie tatsächlich notwendig ist. Oftmals sei aber die Abfrage der Daten die einzige Möglichkeit, um den Sachverhalt aufzuklären und den Täter identifizieren zu können. Teilweise wird von den befragten Richtern und Staatsanwälten geäußert, dass die Polizei die Verhältnismäßigkeit gerade im Hinblick auf den Umfang der Abfrage nach Ort und Zeit nicht immer hinreichend berücksichtige. Teilweise wurde von Seiten der Staatsanwälte angeführt, dass kaum eine mildere Maßnahme als die Verkehrsdatenabfrage denkbar sei. Dagegen führen die Mitarbeiter der Datenschutzbeauftragten an, dass es sich um sensible Daten handle, deren Abfrage u. U. eine stärkere Eingriffsintensität haben könne als die Überwachung des Inhalts der Telekommunikation. Anhand der Daten könnten Neigungen und Interessen nachvollzogen sowie Kontakte

und das soziale Umfeld des Betroffenen festgestellt werden. Zudem entstehe – gerade auch durch die geplante Vorratsdatenspeicherung – ein Gefühl des Überwachtwerdens.

Die Zunahme der Anordnungen nach §§ 100g, 100h StPO erklären sich die Befragten aus Polizei und Justiz vor allem damit, dass die Telekommunikation und die Anzahl der Anschlüsse zugenommen habe. Vor allem die Nutzung von Mobiltelefonen habe sich gesteigert und die Täter würden diese bzw. die SIM-Karten ständig wechseln, um ihre Spuren zu verwischen. Für jeden neuen Anschluss bedürfe es dann eines neuen Beschlusses, was die Anzahl der Beschlüsse in die Höhe treibe. Zudem würde auch die Kriminalität, bei der Telekommunikation eine Rolle spielt, zunehmen. Weitere Gründe für die Zunahme der Anordnungen sei die Kenntnis der Möglichkeit der Verkehrsdatenabfrage durch die Ermittlungsbehörden. Dadurch, dass die Maßnahme schon häufig zum Erfolg geführt hat, würde sie auch immer häufiger eingesetzt.

VI. Durchführung der Maßnahmen

Im folgenden Abschnitt werden die Ergebnisse zur Durchführung der Verkehrsdatenabfrage dargestellt. Der Ablauf innerhalb der Telekommunikationsunternehmen sowie Schwierigkeiten, zu denen es zwischen den Beteiligten gekommen ist, sind Gegenstand der Analyse.

1. Schriftliche Befragung

Die Ergebnisse der schriftlichen Befragung zeigen verschiedene Schwierigkeiten der befragten Staatsanwälte mit den Netzbetreibern auf.

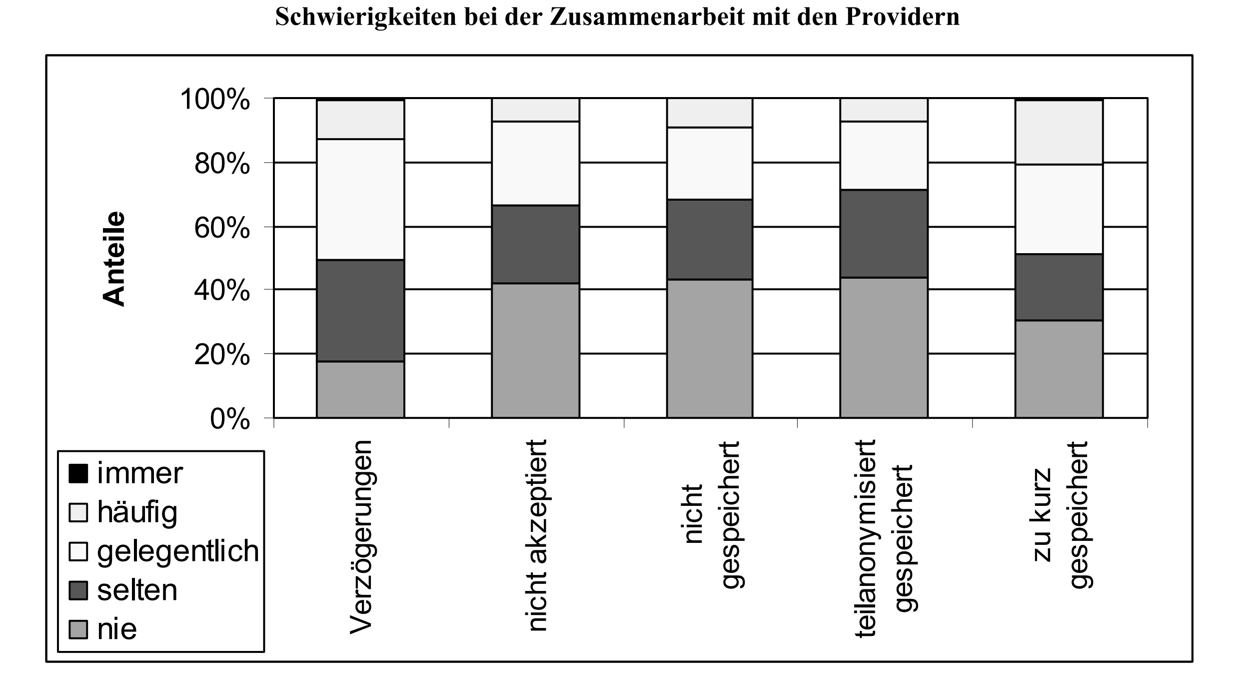
a) Probleme mit den Netzbetreibern

Gelegentliche bis häufige Schwierigkeiten (ca. 50 Prozent der Nennungen) bei der Zusammenarbeit mit den Telekommunikationsanbietern ergaben sich nach Angaben der Befragten vor allem durch Verzögerungen bzw. zu kurze Speicherung der gewünschten Daten (siehe Abbildung 71).

Die Daten waren zum Zeitpunkt der Abfrage häufig bereits gelöscht. Seltener wurden Anordnungen nicht akzeptiert (gelegentlich bis häufig 33 Prozent), die Daten nicht gespeichert (gelegentlich bis häufig 31 Prozent) oder nur teilanonymisiert gespeichert (gelegentlich bis häufig 29 Prozent). Sonstige angegebene Schwierigkeiten beziehen sich auf die unterschiedlich lange Speicherdauer der einzelnen Telekommunikationsanbieter sowie darauf, dass die Verkehrsdatenabfrage am Wochenende nicht durchführbar sei. Weiter wurde kritisiert, dass Anbieter – trotz Ankündigung eines noch zu erwirkenden Beschlusses – die Daten löschten und dass ein gerichtlicher Beschluss verlangt wurde, obwohl ein solcher nicht erforderlich gewesen sei. Ein Drittel der Befragten machte weiterführende Angaben dazu, auf welche Gründe diese Schwierigkeiten zurückzuführen seien. Zum größten Teil kritisierten die Befragten die mangelnde Kooperationsbereitschaft der Provider (16 Prozent derjenigen, die diese Frage beantwortet haben). Die Anbieter würden Desinteresse an der Zusammenarbeit mit den Strafverfolgungsbehörden und der Mitwirkung an der Strafverfolgung zeigen (8 Prozent). Die Durchführung der Abfrage der Verkehrsdaten ist nach dem Eindruck von 4 Prozent dieser Befragten eine „lästige Pflicht“ für die Provider. Zum anderen wurde kritisiert, dass es keine eindeutige Regelung für

Abbildung 71

Schwierigkeiten bei der Zusammenarbeit mit den Providern



eine Speicherfrist gebe (9 Prozent), dass die Provider die Daten unterschiedlich lange speicherten (3 Prozent) und dass diese Dauer der Speicherung bei den Providern zu kurz sei (9 Prozent). Zudem sei die Rechtslage unklar bzw. unzureichend geregelt (8 Prozent). Die Normen seien zu kompliziert und die Rechtsprechung dazu uneinheitlich. Weitere Schwierigkeiten ergäben sich daraus, dass die Anbieter oft eine andere, nach Meinung der Staatsanwälte falsche, Rechtsauffassung hätten (7 Prozent). Es herrsche zudem eine gewisse Rechtsunsicherheit bei den Providern (5 Prozent), die mitunter Angst hätten, etwas Unzulässiges zu tun und sich daher besonders absichern wollten. Außerdem spiele der Datenschutz eine große Rolle (7 Prozent). Die Telekommunikationsanbieter würden ihre Kunden schützen wollen (4 Prozent), wobei einige Staatsanwälte der Ansicht sind, dass sie mit dem Kundenschutz Werbung machen wollen (3 Prozent). 2 Prozent gaben an, dass die Provider immer auf einem Beschluss bestünden und Eilanordnungen der Staatsanwaltschaft nicht akzeptierten. Ein anderes Problemfeld ist nach Angabe der Befragten der hohe Aufwand der Verkehrsdatenabfrage für die Provider. Durch die Masse der Anordnungen seien die Telekommunikationsanbieter überlastet (5 Prozent), die Durchführung der Maßnahme erfordere einen hohen Arbeitsaufwand (3 Prozent) und es käme zu technischen (5 Prozent), personellen (3 Prozent) sowie organisatorischen Problemen (2 Prozent). Auch finanzielle Gründe spielen nach Ansicht der Staatsanwälte für die Anbieter eine Rolle (7 Prozent). Die Anbieter seien wirtschaftlich orientiert (2 Prozent). Weitere Schwierigkeiten ergäben sich daraus, dass Straftaten des Öfteren zu spät bekannt (2 Prozent) und die Maßnahmen zu spät beantragt (2 Prozent) würden. Teilweise seien die Beschlüsse unvollständig oder fehlerhaft und die Ermittlung der richtigen Auskunftsstelle gestalte sich zuweilen als schwierig[448].

Circa 60 Prozent der Befragten machten Angaben darüber, welche Folgen aus den oben genannten Schwierigkeiten resultierten (siehe Abbildung 72). Am häufigsten wurde genannt, dass das Auskunftsersuchen insgesamt erfolglos blieb und Verfahrensverzögerungen entstanden. Dies deckt sich Im Übrigen mit dem eingangs mitgeteilten Forschungsstand sowie mit den Befunden aus der Studie des Bundeskriminalamts aus dem Jahr 2005. Im Einzelnen konnten Beteiligte oder der Beschuldigte nicht identifiziert werden sowie der Anschluss dem Beschuldigten nicht zugeordnet werden.

Die Zusammenarbeit zwischen Staatsanwaltschaft und Polizei bzw. Richtern wurde von den Befragten als gut (58 Prozent) bis sehr gut (36 Prozent) empfunden. Die Beurteilung der Zusammenarbeit mit den Telekommunikationsanbietern schwankt von schlecht (10 Prozent) über mittelmäßig (50 Prozent) bis gut (36 Prozent).

b) Speicherung der Daten

Welche Dauer der Datenspeicherung die befragten Staatsanwälte für angemessen halten, ist in Abbildung 73 dargestellt.

[448] Aufgrund von Mehrfachnennungen summieren sich die genannten Prozentwerte auf über 100 Prozent (hier 126 Prozent).

A b b i l d u n g 72



Folgen der Schwierigkeiten mit den Netzbetreibern

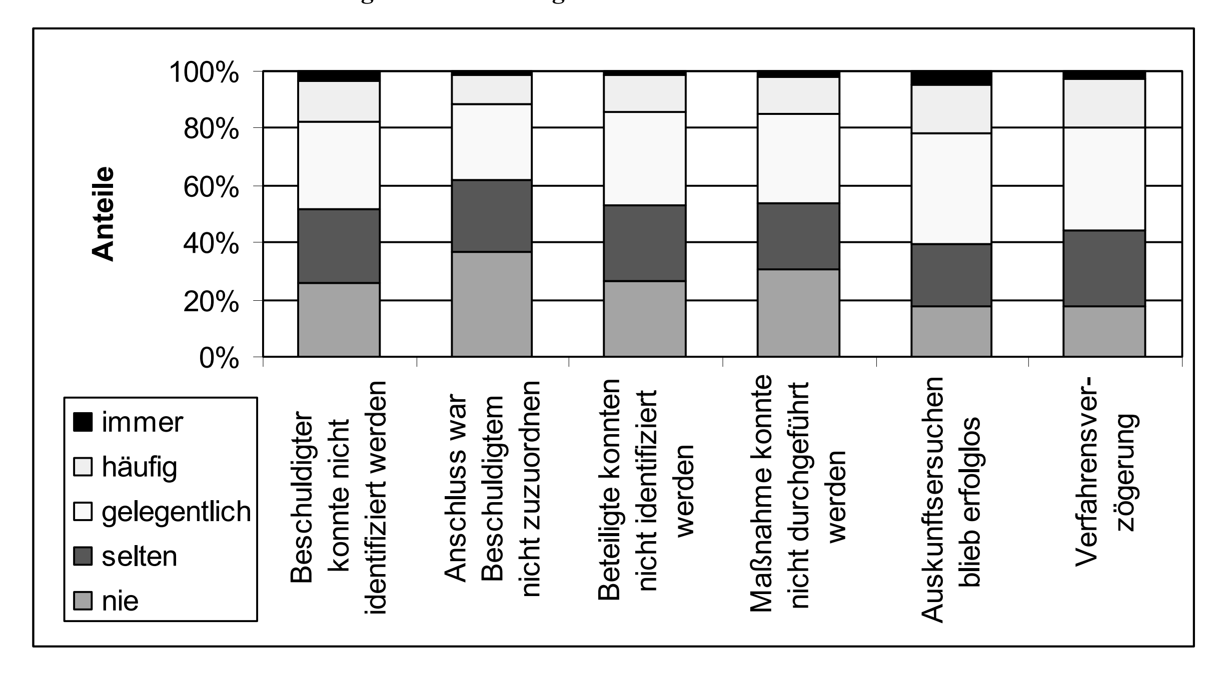
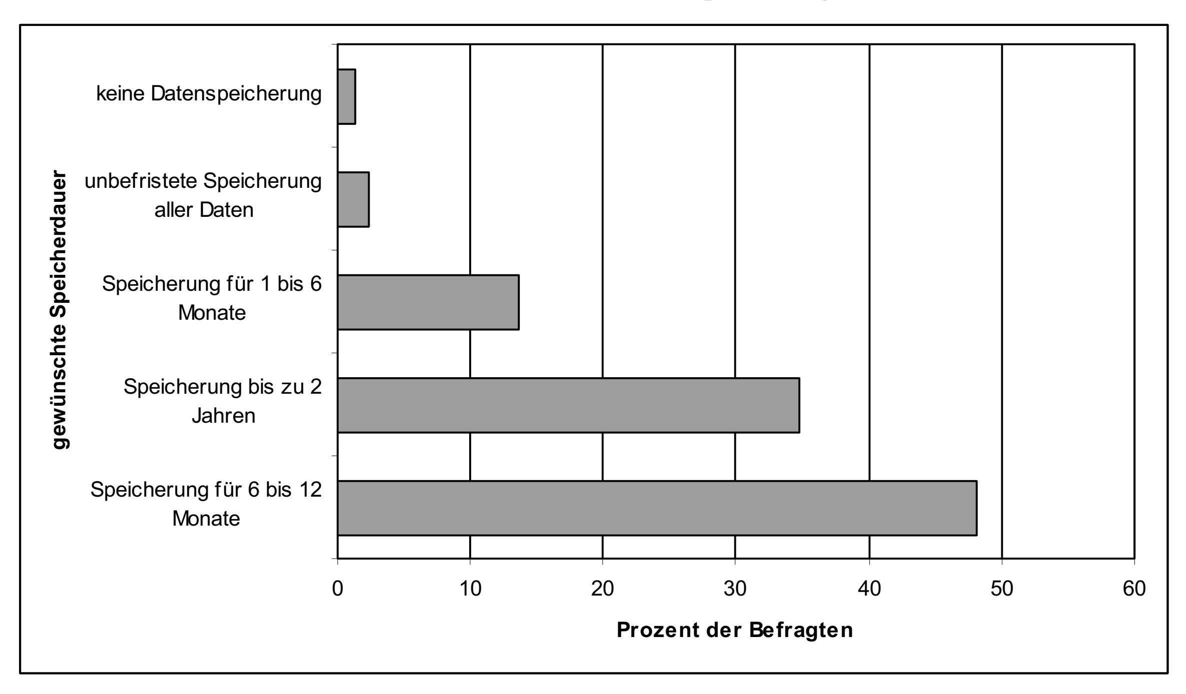


Abbildung 73

Gewünschte Dauer der Datenspeicherung



14 Prozent der Befragten hielten eine Speicherdauer von einem bis sechs Monaten für angebracht, während eine relative Mehrheit (48 Prozent) eine Datenspeicherung von sechs bis zwölf Monate befürwortet. Etwa ein Drittel (35 Prozent) sprach sich für eine Speicherung bis zu zwei Jahren aus. Keine (1 Prozent) oder unbefristete (2 Prozent) Speicherung wurde nur in wenigen Fällen genannt.

c) Schwierigkeiten durch Verschlüsselungstechniken

Verschlüsselungstechniken[449] scheinen keinen großen Einfluss auf die Ermittlungstätigkeit der Behörden zu haben. So gaben 69 Prozent an, dass diese in Ermittlungen noch nie eine Rolle gespielt hätten. Weitere 17 Prozent meinten, dass Verschlüsselungstechniken nur selten eingesetzt würden. 12 Prozent sprachen von einer gelegentlichen Beeinflussung und 2 Prozent davon, dass dies häufiger vorkäme. Bei der Beantwortung gab es keine signifikanten Unterschiede entlang der Dezernate.

Die Frage, in welchem Umfang der Erfolg der Verkehrsdatenabfrage durch Verschlüsselungstechniken beeinträchtigt wurde, wurde von ca. einem Drittel der Befragten beantwortet. Über 50 Prozent von diesen konnten keine Auswirkungen der Verschlüsselungstechniken feststellen. Am häufigsten wurde noch genannt, dass der Beschuldigte nicht identifiziert werden konnte (Abbildung 74). Die anderen Auswirkungen zeigen jedoch sehr ähnliche Verteilungen.

Auch wenn nur die Antworten von Befragten berücksichtigt wurden, die zumindest eine seltene Beeinflussung durch Verschlüsselungen angegeben hatten, zeigte sich keine stärkere Differenzierung zwischen den vorgegebenen Folgen (siehe Abbildung 75).

d) Technische Schwierigkeiten

Eine Beeinträchtigung der Durchführung der Maßnahmen durch technische Probleme kam nach Angaben der Befragten nie (55 Prozent) oder nur selten (29 Prozent) vor. Von gelegentlichen technischen Schwierigkeiten berichteten 14 Prozent. Fast nie wurde von häufigen oder ständigen Problemen berichtet (zusammen 2 Prozent).

[449] Verschlüsselungstechniken wie z. B. anonymisierende Proxys ermöglichen die anonyme Nutzung des Internets. Rückschlüsse auf die Identität der Verwender von IP-Adressen werden durch die Anonymisierungstechniken unmöglich. Zudem ist es möglich, die IP-Adresse eines anderen Nutzers zu manipulieren, so dass dieser anstelle des Täters ins Visier der Strafverfolgungsbehörden gerät. Siehe zum Thema u. a. *Seitz*, 2004, S. 52.

Abbildung 74



Folgen der Verschlüsselung

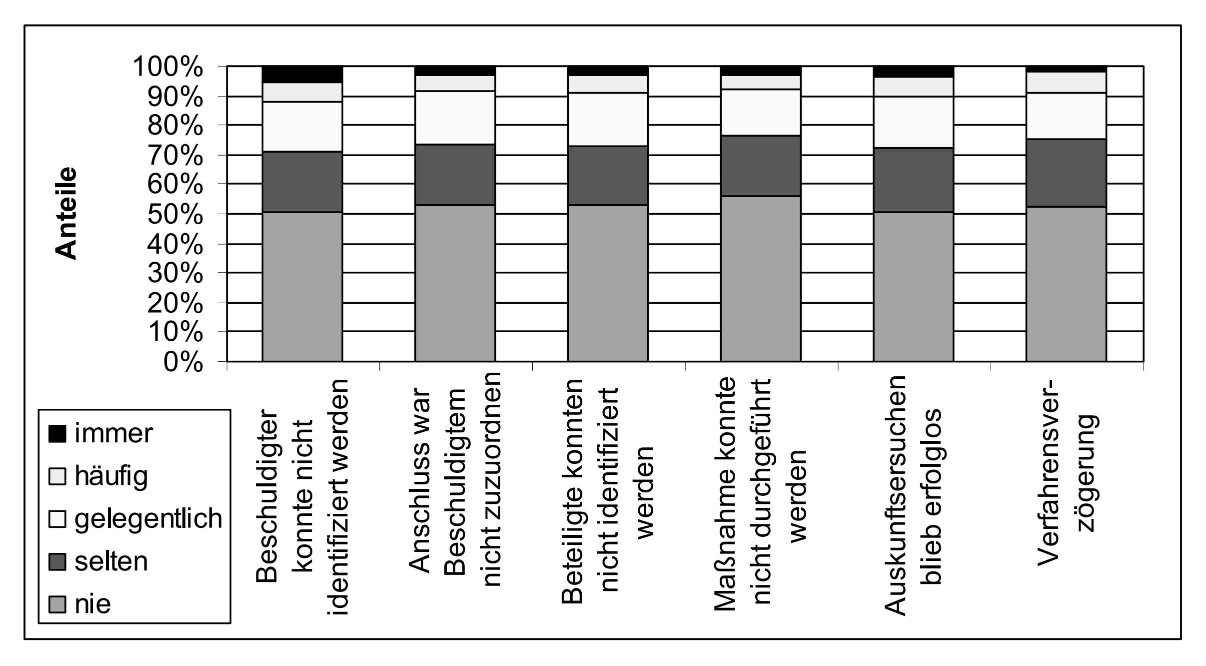
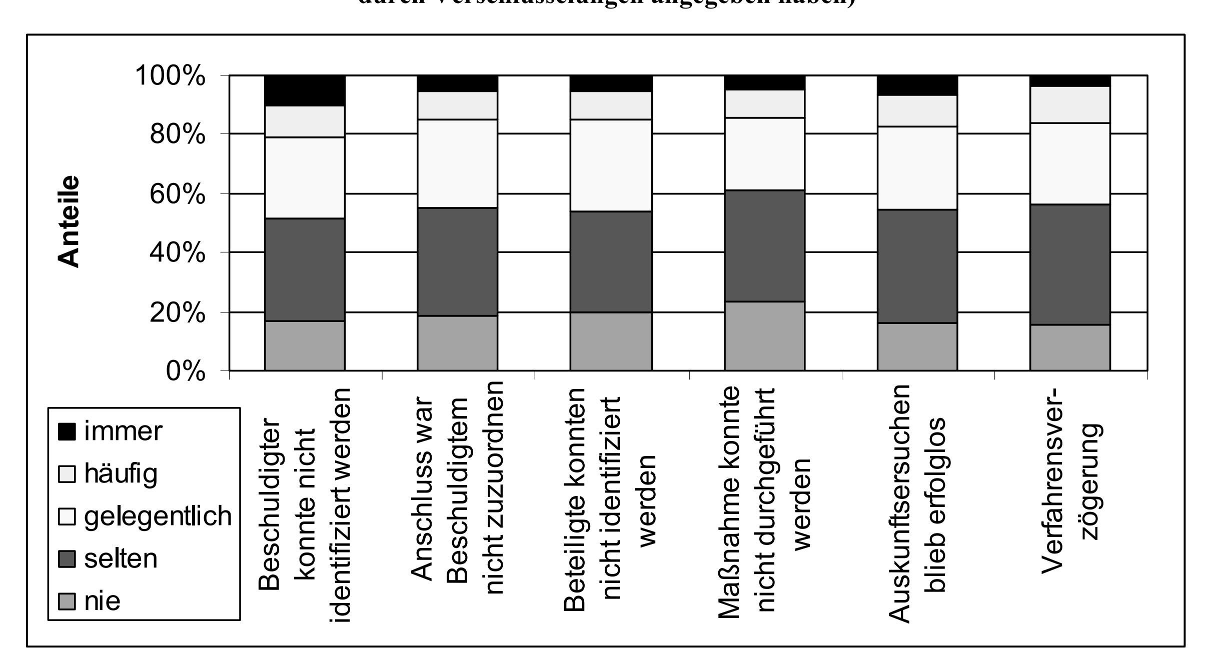


Abbildung 75

Folgen der Schwierigkeiten (Antworten von Befragten, die zumindest eine seltene Beeinflussung durch Verschlüsselungen angegeben haben)



180 der Befragten benannten verschiedene technische Probleme: 30 Prozent gaben an, dass die Daten nicht mehr gespeichert, also bereits gelöscht worden waren. Die Problematik der Speicherung der Daten wurde unter mehreren Gesichtspunkten erwähnt. Einige gaben an, die Daten seien überhaupt nicht gespeichert worden (7 Prozent), die Speicherungsfrist sei abgelaufen gewesen (4 Prozent), die Speicherfristen bzw. -zeiten seien allgemein problematisch (7 Prozent), es sei zu Problemen bei der Speicherung bzw. zur fehlerhaften Speicherung gekommen (8 Prozent) und die Speicherkapazität sei nicht ausreichend gewesen (4 Prozent). 14 Prozent der Befragten, die diese Frage beantworteten, deklarierten allgemein technische Probleme der Anbieter und 4 Prozent Serverabstürze bei den Providern. 7 Prozent gaben Datenverlust an. Als weitere technische Probleme wurden Fehler bei der Übermittlung der Daten (7 Prozent), Übermittlungsverzögerungen (5 Prozent) und Fax-Probleme (z. B. Fax unleserlich, Fax kam nicht an, 5 Prozent) angegeben. 5 Prozent der Antwortenden führten als technisches Problem die mangelnde Erreichbarkeit der Unternehmen an. 4 Prozent bemängelten, dass bei einem Telekommunikationsanbieter eine Auskunft über IMEI-Nummern nicht möglich sei.

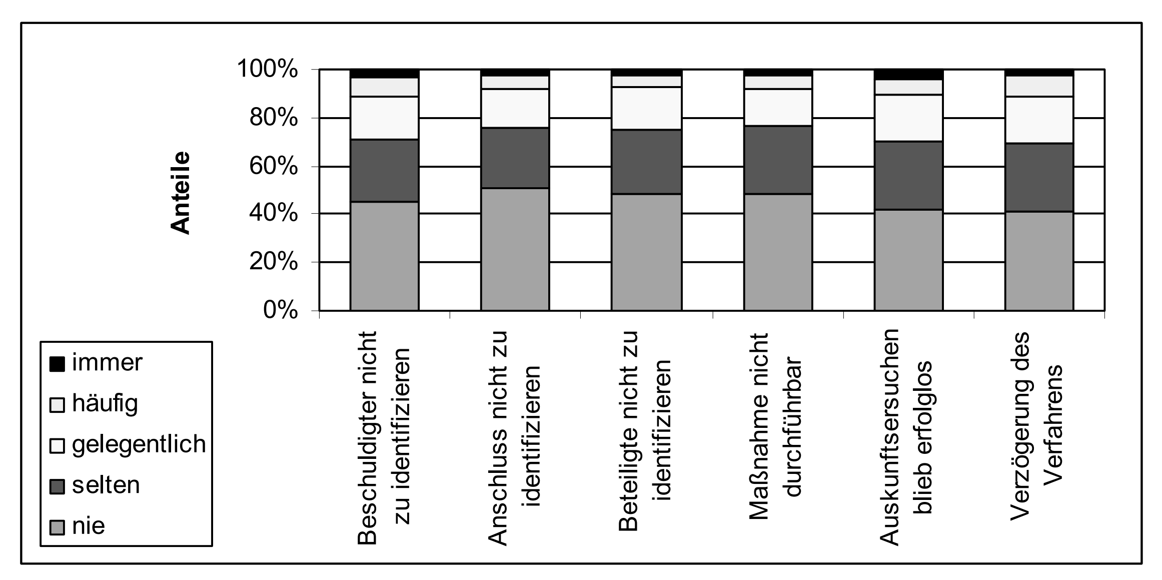
Entsprechend dem selten festgestellten Auftreten technischer Probleme beantworteten nur etwa 320 der Befragten die Frage nach der Erfolgsbeeinträchtigung.

40 Prozent der Befragten gaben keine Folgen der technischen Schwierigkeiten an. Ansonsten waren die Antworten auf die vorgegebenen Kategorien in etwa gleich verteilt (Abbildung 76). Am häufigsten wurden Verfahrensverzögerungen sowie die Erfolglosigkeit des Auskunftsersuchens genannt, gefolgt von der Angabe, dass der Beschuldigte oder weitere Beteiligte nicht zu identifizieren und die Maßnahmen nicht durchführbar waren. Schließlich wurde auch angegeben, dass der Anschluss des Beschuldigten nicht festgestellt werden konnte.

Abbildung 76



Folgen von technischen Problemen



2. Aktenanalyse

Bei der Auswertung der Verfahrensakten konnten verschiedene Einflussfaktoren im Hinblick auf die Durchführung der Maßnahme festgestellt werden.

a) Nichtakzeptierung von Anordnungen und Verzögerungen

Bei 27 Beschlüssen haben Telekommunikationsanbieter die Herausgabe der Verkehrsdaten ausdrücklich verweigert. Zum größten Teil betrifft dies Fälle, in denen eine staatsanwaltschaftliche Eilanordnung erfolgte. Die Anbieter forderten einen die Anordnung bestätigenden richterlichen Beschluss, damit die Daten herausgegeben werden (elf Fälle). Weiterer Verweigerungsgrund war die Fehlerhaftigkeit der Beschlüsse (acht Fälle). In diesen Beschlüssen waren falsche oder unvollständige Rufnummern angegeben, der angeschriebene Anbieter gar nicht in dem Beschluss als Verpflichteter aufgeführt und keine oder nicht die aktuelle Rechtsgrundlage genannt. In zwei Fällen verlangte der Anbieter einen Beschluss anstelle einer einfachen Anforderung. In einem Fall ist der erlassene Beschluss nicht beim Anbieter angekommen und deswegen wurde keine Auskunft erteilt. In den übrigen fünf Fällen war kein Grund für die Weigerung ersichtlich. Zu Verzögerungen ist es in diesen Fällen nur teilweise gekommen. In sieben Fällen führte das Warten auf die richterliche Bestätigung der Eilmaßnahmen zu Zeitverzögerungen. In beiden Fällen, in denen ein Beschluss anstelle einer einfachen Anforderung gefordert wurde, kam es zu Verzögerungen. In fünf Fällen wurde aufgrund der Fehlerhaftigkeit des Beschlusses ein neuer Beschluss erlassen. Abgesehen von der eher umstrittenen Frage der Herausgabe der Daten bei Eilanordnungen, beruhte die Weigerung – soweit ersichtlich – auf der Fehlerhaftigkeit der Anforderungen. In diesen Fällen wurden keine Ordnungs- und Zwangsmittel seitens der Justizbehörden verhängt. Nur in einem Fall wurde eine solche Maßnahme von der Staatsanwaltschaft beim Richter beantragt, aber letztendlich nicht durchgesetzt. In keinem Fall wurde seitens der Diensteanbieter Beschwerde gegen einen Beschluss eingelegt.

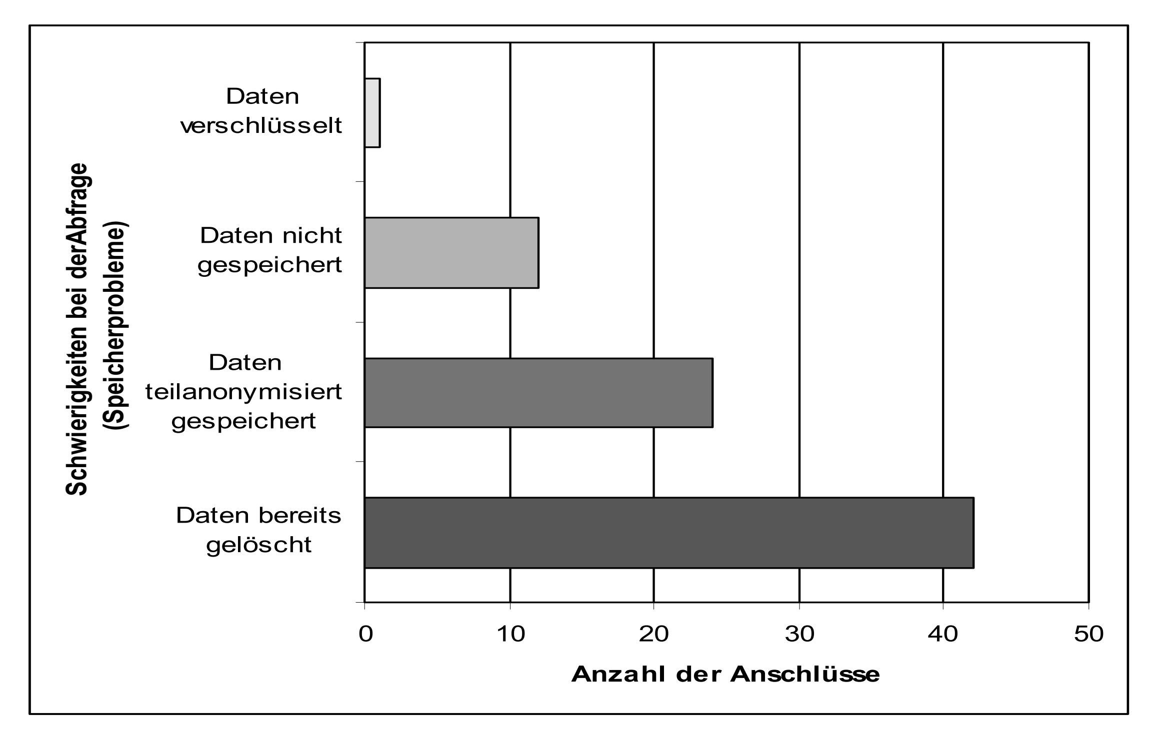
Zu sonstigen Verzögerungen ohne explizite, den Akten zu entnehmende Weigerung der Anbieter, kam es in 32 Fällen. In acht Fällen beruhte dies darauf, dass der Beschluss fehlerhaft war, wobei vor allem eine falsche Ruf- oder IMEI-Nummer die Fehlerhaftigkeit begründete (fünf). Daneben gab es einen Fall, in dem kein Abfragezeitraum genannt wurde und zwei Fälle, in denen der Beschluss nicht eindeutig war. Weitere Gründe für eine zeitliche Verzögerung waren, dass die Zustellung des Beschlusses nicht erfolgte bzw. an einen falschen Empfänger ging (drei) und dass das Anschreiben fehlerhaft war oder fehlte (zwei). Verzögerungen durch die Netzbetreiber ergaben sich u. a. dadurch, dass eine zeitgerechte Antwort wegen Personalmangels nicht möglich war (zwei) und dass falsche Daten abgefragt wurden (drei).

b) Löschung von Daten und (teil)anonymisierte Daten

Bei 4 Prozent der Anschlüsse kam es zu Problemen hinsichtlich der Speicherfristen bzw. der Speicherart (siehe Abbildung 77).

Abbildung 77


Schwierigkeiten bei der Abfrage wegen Speicherung



Die Probleme konzentrieren sich offensichtlich auf die kurze Speicherungsdauer und die damit verbundene Löschung von Verkehrsdaten (42 Anschlüsse). Weniger häufig war die Abfrage der Daten dadurch beeinträchtigt, dass die Daten teilanonymisiert gespeichert waren (24). Bei zwölf Anschlüssen waren die Daten von vornherein nicht bei den Anbietern gespeichert (z. B. bei Prepaid-Anschlüssen). Bei einem der Anschlüsse waren die Daten verschlüsselt. Diese Probleme tauchten in 64 Beschlüssen auf, wobei in manchen Beschlüssen die Probleme mehrere Anschlüsse betrafen. Sie verteilen sich dabei in nahezu gleicher Weise wie auf die Anschlüsse, so dass auf die beschlussbezogene graphische Darstellung verzichtet wird. Die Daten waren bei 37 Beschlüssen zum Zeitpunkt der Abfrage bereits gelöscht. Bei 17 Beschlüssen waren die Daten nur teilanonymisiert gespeichert, bei neun Beschlüssen waren die Daten von vornherein nicht gespeichert und ein Beschluss war mit verschlüsselten Daten konfrontiert.

Die Aktenanalyse führt somit zu dem Ergebnis, dass im Untersuchungszeitraum die Löschung im Zusammenhang mit der Ausführung der Verkehrsdatenabfrage jedenfalls keine erhebliche Rolle spielt. Bereits erfolgte Löschungen betreffen etwa 2 Prozent der durch die Anordnungen erfassten Anschlüsse. Freilich wird dabei nicht erkennbar, inwieweit Entscheidungen zur Antragsstellung und zur Anordnung durch die Überlegung beeinflusst werden, dass voraussichtlich auf Daten nicht mehr würde zurückgegriffen werden können. Jedoch dürfte sich das Entscheidungsverhalten von Staatsanwälten und Richtern an die Speicherungs- und Löschungspraktiken der Telekommunikationsunternehmen angepasst haben.

Die auf die Speicherung bezogenen Probleme haben sich teilweise auf den Erfolg der Verkehrsdatenabfrage ausgewirkt. Bei 13 Anschlüssen, bei denen die Daten zum Zeitpunkt der Abfrage bereits gelöscht waren, konnten erwartungsgemäß keine Erfolge mit der Verkehrsdatenabfrage erzielt werden. Die Anordnung ging ins Leere. Bei den Anschlüssen, bei denen die Daten teilanonymisiert gespeichert waren, konnte nur bei einem dieser Anschlüsse den Akten explizit entnommen werden, dass der mangelnde Erfolg auf die Teilanonymisierung zurückzuführen ist. Im Übrigen war den Akten nur zu entnehmen, dass keine relevanten Erkenntnisse gewonnen werden konnten. In den Fällen, in denen die Daten von vornherein nicht gespeichert waren, konnte bei drei Anschlüssen eindeutig festgestellt werden, dass die Erfolglosigkeit der Ermittlungen auf die fehlenden Daten zurückzuführen war.

Nur in einem Fall war den Akten ein Hinweis auf verschlüsselte Daten zu entnehmen. Es konnte freilich kein Hinweis darauf gefunden werden, dass die Anonymisierung die Ermittlungen beeinflusst hat. Es ist anzunehmen, dass Verschlüsselungsprobleme eher im Bereich des Internets auftreten. In den ausgewerteten Verfahren (aus den Jahren 2003 und 2004) wurden jedoch ganz überwiegend Daten von Telefonen und Handys abgefragt. Nur in 14 Fällen wurden Daten zu IP-Adressen abgefragt. Diese Abfragen betrafen acht Verfahren. Wie die Daten zur Anzahl der Abfragen zu IP-Adressen, die von T-Com zur Verfügung gestellt wurden, zeigen, fand ein starker Anstieg der Abfragen erst 2005 statt.

c) Technische Probleme

Den Akten konnten nur in Einzelfällen technische Schwierigkeiten entnommen werden. Dabei handelte es sich in zwei dieser Fälle darum, dass den Anbietern die Ausführung des Beschlusses rein technisch gesehen nicht möglich war. Es handelte sich also nicht um vorübergehende technische Probleme, sondern um Fälle, in denen die Anbieter oder ein einzelner Anbieter prinzipiell nicht in der Lage waren, dem Beschluss technisch nachzukommen. In einem Fall ist allgemein davon die Rede, dass ein Anbieter in Bezug auf einen Anschluss technische Probleme bei der Ausführung hatte. Welcher Art genau diese Probleme waren, konnte den Akten nicht entnommen werden.

3. Experteninterviews

a) Telekommunikationsunternehmen

(1) Geschäftsablauf

Der Geschäftsablauf bei der Durchführung von Verkehrsdatenabfragen wurde von allen Telekommunikationsanbietern ähnlich dargestellt. Die Anfragen würden per Post, Fax oder E-Mail eingehen. Die eingehenden Anfragen würden dann nach der Art von Abfragen (Verkehrsdatenabfragen, die in die Vergangenheit oder in die Zukunft gerichtet sind; Funkzellenabfragen; Bestandsdaten) sortiert. Im Anschluss hieran erfolge eine Überprüfung, ob der Beschluss richtig bzw. auch an den richtigen Adressaten gerichtet und ob er technisch umsetzbar sei. Es werde schließlich geprüft, welche Daten der Anfragende genau verlange. Der Beschluss bzw. die Anfrage werde eingescannt oder eingegeben und die nachfolgende Bearbeitung erfolge dann in elektronischer Form. Dabei haben die Anbieter unterschiedliche Systeme (Datenpools) eingerichtet, mit denen die Daten abgefragt werden. Der Sachbearbeiter starte den Vorgang und überprüfe, ob der Suchlauf ordnungsgemäß ablaufe. Dann würden die Daten auf CD-Rom gebrannt oder ausgedruckt und per Fax, E-Mail (verschlüsselt) oder (wenn dies gewünscht wird) auf Diskette oder CD-Rom verschickt. Der Mitarbeiter eines Unternehmens erläuterte, dass der Vorgang unterschiedlich sei, je nachdem ob das Festnetz oder das Internet betroffen sei. Je nachdem, welche Daten abgefragt würden, würden unterschiedliche Prozesse gestartet. Wenn abgehende Daten abgefragt werden, erhielten die anfragenden Stellen eine Kopie des Einzelverbindungsnachweises. Wenn „ankommende“ Daten abgefragt würden, werde ein Zielwahlsuchlauf gestartet. Die Abfrage zukünftiger Daten sei überwiegend überwachungstechnisch ausgestaltet. Es würden fortlaufende Ereignisdaten gesendet. Der vierte Anwendungsbereich seien die Personendaten zu dynamischen IP-Adressen.

Daneben gibt es zwei Anbieter, die an eine elektronische Schnittstelle für Behörden (ESB) angeschlossen sind. Die Elektronische Schnittstelle für Behörden(anfragen) (ESB)

beinhalte nach Angaben dieser Anbieter elektronische Anfragen und elektronische Beauskunftung. Dieser Schnittstelle würden sich in Nordrhein-Westfalen der Zentrale Polizeidienst Duisburg und in Bayern das Bayerische Landeskriminalamt bedienen. Es handle sich um einen „elektronischen Rückkanal“. Bei der Polizei werde ein zentraler Abfrageort eingerichtet, über den alles abläuft. Das Projekt befinde sich zur Zeit noch in der Testphase. Eine Kommission (KomGüt) bemühe sich derzeit darum, dies bundesweit zu verbreiten. Die ESB sei aus dem Wunsch der Netzbetreiber nach möglichst wenig Ansprechstellen entstanden. Es würde sich dann nur eine zentrale Stelle um diese Angelegenheiten kümmern. Einer der befragten Mitarbeiter eines der bereits teilhabenden Unternehmen gibt an, dass der Wunsch bestehe, dass sich weitere Unternehmen und Länder an diesem Projekt beteiligen. Eine gesetzliche Verpflichtung zur Beteiligung sei jedoch – gerade für kleinere Anbieter mit wenigen Anfragen – unangemessen. Bei den Anbietern, die die Schnittstelle bereits nutzen, entstehen insoweit zwei Prozesse: Entweder kommt die Anfrage auf dem normalen Postweg oder über die Elektronische Schnittstelle für Behörden. Wenn eine Anfrage per Post kommt, gestaltet sich der Ablauf wie oben dargestellt. Wenn eine Anfrage über die ESB ankommt, wird ein elektronischer Beschluss geschickt und das Original kommt auf dem Postwege nach. Es erfolgt dann (bei ESB) eine reine Plausibilitätsprüfung (ob die Nummer vergeben ist, etc.). Dann wird der Vorgang wie auf dem normalen Wege gestartet und der Versand des Ergebnisses erfolgt wieder über die Schnittstelle. Diese elektronische Schnittstelle für Behörden wird von den befragten Mitarbeitern der Unternehmen unterschiedlich beurteilt. Die Befragten, dessen Unternehmen bereits an ESB angeschlossen sind, meinen, dass die Vorteile darin zu sehen seien, dass die Personen, die damit beschäftigt sind (Polizisten), über gute Kenntnisse technischer und rechtlicher Art verfügen. Außerdem erfolge eine zentralisierte Abrechnung. Die Unternehmen müssten dann nur eine Sammelrechnung erstellen und auch das Landeskriminalamt hätte nur mit dieser Sammelrechnung zu tun. So müssten nicht ständig Einzelrechnungen i. H. v. jeweils 20 Euro erstellt werden, was einen erheblichen Aufwand und erhebliche Kosten bedeute. Das Verfahren über den Postversand bedeute einen großen Aufwand und koste zudem mehr Geld als die elektronische Vorgehensweise. Ein anderer Befragter sieht dagegen nur einen relativ geringen Rationalisierungseffekt. Die Beschlüsse müssten weiterhin geprüft werden. Vorteile seien jedoch, dass Fehleingaben auf Seiten der Unternehmen minimiert werden könnten. Fehleingaben durch die Bedarfsträger seien jedoch weiterhin möglich. Weiterer Vorteil sei zudem fachkundiges Personal der Polizei. Zwei weitere Befragte halten die Automatisierung für rechtlich bedenklich. Der Direktzugriff des Bedarfsträgers auf Daten sei kritisch zu betrachten. Die berechtigte Behörde zur Abfrage sei bei der ESB die Polizei. Die Polizei würde dann eine Anfragemaske mitschicken, die das Unternehmen „durchwinken“ und zur automatischen Datengenerierung führen könne. Dadurch würde die Kontrolle über die Daten aus der Hand genommen. Sie seien aber zur Wahrung des Fernmeldegeheimnisses verpflichtet und hätten Verantwortung gegenüber ihren Kunden. Gegenüber dem bisherigen System seien keine Vorteile zu sehen. Die Behörden, die die Daten elektronisch übersandt haben wollten, würden die Daten per Mail (verschlüsselt mit PGP) oder auf Diskette gespeichert geschickt bekommen.

Alle befragten großen Anbieter schildern, dass sie eine Abteilung für Auskunftsersuchen der Behörden hätten bzw. dass dies ein Teil einer größeren Abteilung sei. In diesen Abteilungen sind sieben bis 18 Mitarbeiter beschäftigt. Meist werden in den Abteilungen neben Verkehrsdatenabfragen Auskünfte über Bestandsdaten erteilt und Telekommunikationsüberwachungsmaßnahmen bearbeitet.

(2) Prüfungsrecht der Telekommunikationsunternehmen

Wie bereits ausgeführt ist es umstritten, inwiefern die Diensteanbieter die Beschlüsse überprüfen müssen oder dürfen. Ob die Beschlüsse überwiegend ohne Gründe geschickt werden, beantworteten die Befragten unterschiedlich. Drei der befragten Unternehmensmitarbeiter gaben an, dass sie die Beschlüsse zumeist mit Begründung erhalten. Drei Befragte meinen, dass dies von Gericht zu Gericht unterschiedlich sei.

Alle Befragten gaben an, dass die formellen Voraussetzungen der Anordnungen von den Sachbearbeitern geprüft würden. Bei Zweifeln würden sie sich an die Rechtsabteilung wenden. Es werde u. a. geprüft, ob der Richterwille eindeutig ist und ob z. B. falsche Angaben gemacht wurden. Es werde auch geprüft, ob eine zu lange Frist angeordnet wurde. Eine inhaltliche Prüfung fände nicht statt, meint einer der Befragte. Die materielle Prüfung sei gesetzlich nicht erlaubt. Zwei Befragte geben an, dass sie bzgl. der materiellen Voraussetzungen Erwägungen dahingehend anstellen würden, ob die Maßnahmen verhältnismäßig sind. Dazu fühlten sie sich verpflichtet. Diesbezügliche Beschwerden würden aber nicht zum Erfolg führen und mit der Begründung abgelehnt werden, dass sie kein Prüfungsrecht hätten. Da durch Beschwerden Kosten entstehen, legen sie diesbezüglich auch keine Beschwerden mehr ein. Drei Befragte gaben an, dass sie auch die materiellen Voraussetzungen prüfen. Sie hätten auch schon mal Anfragen wegen einem einfachen Diebstahl wegen Unverhältnismäßigkeit abgelehnt.

(3) Zeitaufwand für die Durchführung

Welchen Zeitaufwand eine Auskunftserteilung für die Unternehmen bedeute, wurde unterschiedlich beantwortet. Ein Befragter gibt an, dass die Bearbeitung 20 bis 25 Minuten bei ein bis zwei Rufnummern dauere. Ein anderer Befragter schildert, dass das Eingeben und Anlegen des Vorgangs 30 Minuten dauere. Bei Zielwahlsuche und Funkzellenabfrage handle es sich um ein zeit- und arbeitsintensiveres Vorgehen. Das seien Prozesse, die weit über eine Stunde dauern würden. Dies hänge u. a. davon ab, ob die Örtlichkeit bekannt sei oder nicht. Des Weiteren wurde von einem Befragten angegeben, dass der Ar-

beitsaufwand bei bis zu vier Rufnummern unter einer Stunde betragen würde. Im Durchschnitt beinhalte eine Anfrage vier Rufnummern. Im Durchschnitt würden zehn bis 60 Minuten benötigt. Wie hoch der Aufwand ist, hänge auch davon ab, wie genau der Beschluss formuliert sei. Das steigere sich je nachdem, wie viele Rufnummern, IMEIs es sind. Ein anderer Befragter schildert, dass in einer Stunde drei Funkzellenabfragen erfolgen würden oder fünf Verkehrsdatenabfragen, d. h. Abfragen für fünf Rufnummern. Der Arbeitsaufwand sei unterschiedlich, gibt ein anderer Befragter an. Es dauere etwa 55 Minuten bei einer normalen Abfrage, bei der Zielwahlsuche etwa 1 Std. 15 Minuten. Eine Maßnahme könne aber auch mal 15 Minuten dauern. Ein weiterer Befragter gibt als Durchschnittswert pro Beschluss 1,5 Stunden an.

(4) Probleme bei der Zusammenarbeit mit Polizei und Justiz

Es wurden verschiedene Schwierigkeiten bei der Zusammenarbeit mit den Polizei- und Justizbehörden seitens der Mitarbeiter der Unternehmen aufgeführt. Zum einen wurde angegeben, dass die Behörden nicht nachvollziehen könnten, dass in einem Unternehmen Daten vorhanden sind, die ein anderes Unternehmen nicht speichert. Man versuche sie dann gegeneinander auszuspielen, in dem behauptet wird, dass andere Unternehmen das aber auch könnten. Andere Unternehmen hätten aber andere Arbeitsweisen. Ein weiteres Problem seien die mangelnde Fachkompetenz und die Unwissenheit der Behörden. Paragraphen würden von Staatsanwaltschaft und Gericht vermischt und es würden Voraussetzungen in die Paragraphen hineininterpretiert, die man aus §§ 100g, 100h StPO nicht entnehmen könne. Es herrsche ein Halbwissen über die rechtlichen Voraussetzungen. Darüber würden dann diverse telefonische Diskussionen geführt. Zudem sei auch eine technische Unkenntnis zu bemerken. Die Behörden würden teilweise Maßnahmen verlangen, die technisch nicht möglich seien. Auch würden die Behörden die datenschutzrechtlichen Vorschriften nicht kennen, gibt dieser Befragte weiter an. Sie könnten nicht verstehen, wenn Daten nicht mehr gespeichert sind. Dies sei jedoch von den Kundenwünschen abhängig. Der Großteil der Kunden habe die Speicherung untersagt.

Zudem sei die Lesbarkeit von Beschlüssen problematisch, führt ein Befragter aus. Die Fax-Übermittlung lasse zu wünschen übrig. Außerdem seien Beschlüsse häufig schwer zu verstehen. Man müsse schon über gewisse Erfahrungen verfügen, um zu interpretieren, was gewollt ist. Sie seien ungenau und unpräzise. Es würden unklare Formulierungen gewählt, ob die abgehenden oder ankommenden Daten angefragt werden sollen. Man müsse aus dem Delikt herauslesen, was gewollt ist. Man interpretiere die Beschlüsse, um zu erfahren, was abgefragt werden soll. Teilweise seien die Dienststellen nicht in der Lage, die Daten entgegenzunehmen, weil sie so umfangreich sind.

Problematisch sei zudem, dass auf Eilanordnungen keine richterliche Bestätigung erfolge oder diese erst nach den vorgeschriebenen drei Tagen erfolge. Dies sei vor allem bei Abfragen von Vergangenheitsdaten der Fall. Dann seien die Daten ja abgefragt worden und die Sache habe sich für die Behörden erledigt. Ein Befragter meint, er fordere auf eine Eilanordnung hin einen Beschluss. Die Staatsanwaltschaft müsse das Merkmal der Gefahr im Verzug erläutern. Sie würden sich an die Rechtsprechung halten, die Justiz dagegen nicht. Die Polizei reagiere teilweise mit Unverständnis auf die Forderung eines Beschlusses. Die Daten würden aber nicht ohne Beschluss herausgegeben. Ein anderer Befragter berichtet, dass früher darauf beharrt worden wäre, die richterliche Bestätigung innerhalb von drei Tagen zu erhalten. Ihnen sei aber mitgeteilt worden, dass die Bestätigung nur erforderlich sei, wenn die Abfrage in die Zukunft erfolge. Gegen diese Auslegung spreche aber der Wortlaut der Normen und auch die Regelung bei §§ 100a, 100b StPO. Ein Befragter berichtet davon, dass die Polizei Verkehrsdaten ohne Beschlüsse wolle. Darauf ließen sie sich aber nicht ein.

Früher seien die Bestandsdaten zur IP-Adresse nur mit Beschluss nach §§ 100g, 100h StPO herausgegeben worden. Mittlerweile würden diese nach § 113 TKG herausgeben, da es entsprechende Urteile gegeben habe. Seitdem seien weniger Anfragen zu beobachten und kontroverse Diskussionen nähmen ab. Die Abfrage dynamischer IP-Adressen sei weiterhin problematisch, meinen drei andere Befragte. Die Befragten halten eine Beschluss nach §§ 100g, 100h StPO bei der Abfrage von Personendaten zu dynamischen IP-Adressen für erforderlich. Begründet wird dies u. a. damit, dass sie diese Daten aus dem Billingsystem gewinnen müssen. Die Begründung, dass die IP-Adressen schon vorlägen und nur noch der Name benötigt werde, sei oberflächlich. Die Daten könnten nur über Verkehrsdaten ermittelt werden, erläutert ein anderer Befragter. Wenn ein Beschluss nach §§ 100g, 100h StPO (von einem LG) abgelehnt würde, würde eine Notlösung über § 161a StPO führen. Bisher habe sich noch kein OLG damit beschäftigt, aber es gebe LG-Urteile für beide Auffassungen. Die Rechtsprechung werde hier uneinheitlich praktiziert.

Ein weiteres Problem sei das Ermitteln von Cash-Card-Aufladungen. Bei den Aufladungen habe Telekommunikation stattgefunden. Für die Daten, wann die Karten aufgeladen wurden, bedürfe es daher auch eines Beschlusses. Ein anderer Befragter schildert, dass das Aufladen von Prepaidkarten ein Diskussionspunkt sei. Die Auskunft, welcher Rufnummer das Guthaben der gestohlenen Prepaid-Karten gutgeschrieben wird, sei ebenfalls ein Telekommunikationsvorgang und betreffe das Fernmeldegeheimnis. Um die Daten zu erlangen, müssten die gesamten Verbindungen durchsucht werden. Auch hierfür bedürfe es eines Beschlusses. Probleme würden sich auch bei der Beauskunftung von Standortdaten des Mobiltelefons im „Stand-by-Betrieb“ ergeben, meint einer der Befragten. Von einer „Zusammenarbeit“ könne man eigentlich nicht sprechen, führt ein weiterer Befragter aus. Es herrsche eine Waffenungleichheit. Je weniger Chancen für die Übermittlung von Daten bestünden, desto aggressiver würden Staatsanwaltschaft und Polizei reagieren. Es würden nach der Meinung dieses Befragten weniger Be-

schlüsse erlassen, wenn die Kostentragung anders geregelt wäre, d. h. wenn die Justiz die Kosten tragen müsste.

Ein weiteres Problem sei, dass die Behörden mit Unverständnis darauf regieren würden, dass keine eingehenden Daten gespeichert werden, schildert ein Festnetzanbieter. Gespeichert würden aber nur abgehende Daten. Die eingehenden Daten würden keine Kosten verursachen. Die Anrufer bekämen keine Rechnung, daher würden auch ihre Daten nicht gespeichert. Beim Zielwahlsuchlauf würden dann alle, also Millionen von Kunden daraufhin gerastert, ob sie eine bestimmte Nummer angerufen haben. Da nur die Fernmelderechnungsdaten der Kunden gespeichert seien, könnten auch nur die Daten der Kunden des Unternehmens ermittelt werden. Die Justiz interpretiere, wenn keine Daten gespeichert wurden, dies aber so, dass keiner angerufen habe. Es seien aber nur an einer Stelle keine Daten entstanden. Der Zielwahlsuchlauf werde also nicht verstanden von Staatsanwälten, Richtern und Polizisten. Das Ausmaß des Grundrechtseingriffs sei ihnen nicht bewusst. Die Maßnahme ähnle einer Rasterfahndung. Von einem Anbieter werden keine Schwierigkeiten berichtet. Hier heißt es, es verlaufe Alles reibungslos.

Vier der befragten Unternehmensmitarbeiter geben an, dass die Anfragen häufig bzw. immer als dringend dargestellt werden. Dahinter stecke der Ermittlungsdruck. Es werde regelmäßig um bevorzugte Behandlung gebeten. Einer der Befragten meint, dass in regelmäßigen Abständen angerufen würde, wenn es wirklich dringend sei. Fast jedes Anschreiben stelle die Datenabfrage als besonders dringend dar. Ein Befragter meint, dies sei zu 50 Prozent der Fall, aber die Tendenz sei steigend.

(5) Anforderung der Daten ohne Beschluss

Gelegentlich versuche die Polizei die Daten (ohne Beschluss) von den Unternehmen zu erfragen, gaben vier der Befragten an. Darauf würden sie sich jedoch nicht einlassen. Ein Befragter führte aus, dass es häufiger vorkomme, dass Auskünfte zu dynamischen IP-Adressen aufgrund einer banalen Rechtsgrundlage erfragt würden. Ein Befragter meint, dass dies nicht vorkomme. Aber die Sachbearbeiter würden sehr oft Beratungsleistung erbringen. Es würde gefragt, was getan werden müsse, um die Daten zu erlangen und ob es eines §§ 100g, 100h StPO-Beschlusses bedürfe. Die Sachbearbeiter würden also vielfach über die technischen Gegebenheiten, aber auch die rechtlichen Voraussetzungen aufklären. Ein anderer Befragter schildert ein weiteres Problem. Die Behörden würden Einverständniserklärungen von Kunden vorlegen und die Daten verlangen. Dies sei jedoch eine Ignoranz des Fernmeldegeheimnisses des Gesprächspartners des Kunden. Sie würden nur auf Anfragen von Behörden antworten. Die Beauskunftung des Kunden über Verkehrsdaten sei gesetzlich nicht vorgesehen.

(6) Weigerungen der Diensteanbieter

Die Mitarbeiter von drei der Diensteanbieter gaben an, dass sie sich im Jahr 2005 nicht geweigert hätten, Beschlüsse auszuführen oder Beschwerden gegen Anordnungen eingelegt hätten. Ein Befragter meint, wenn es Probleme gebe, würden sie das mit den Behörden klären. Ein anderer Befragter gab an, dass sie sich in der Regel nicht weigern würden, da das Risiko zu groß sei. Ein Befragter meint, Beschwerden seien die Ausnahme, weil sie bisher kaum erfolgreich waren und nur Kosten entstanden seien. Ein Befragter gibt an, dass im Jahr 2005 eine Beschwerde eingelegt worden sei. Zu einer Verweigerung der Abfrage komme es nicht, da die Beschlüsse ausgeführt werden müssten. Im Jahr 2005 seien drei Beschwerden eingelegt worden, gibt ein anderer Befragter an. Alle Beschwerdeverfahren seien zum Nachteil der Unternehmen ausgegangen. Es habe fünf bis sechs inoffizielle Beschwerden und keine Weigerung gegeben. Man müsse es sich als Unternehmen überlegen, wie viel Zeit und Geld in ein solches Vorgehen gesteckt werde, vor allem, wenn zu erwarten sei, dass die Sache nicht von Erfolg gekrönt sein werde. Ein weiterer Befragter schildert, dass im Jahr 2006 drei Beschwerden eingelegt worden seien. Diese hätten sich auf Massenzellanfragen bezogen. Es sollten Daten aus über 90 Funkzellen in stark frequentierten Bereichen über einen längeren Zeitraum abgefragt werden. Die Beschwerden seien aber abgelehnt worden.

(7) Ordnungs- oder Zwangsmittel und Strafverfahren wegen Strafvereitelung

Mit Ordnungs- oder Zwangsmitteln wurden – abgesehen von einem Fall (Zwangsgeld) – die Befragten im Jahr 2005 nicht belegt. Gegen drei der Unternehmen wurden keine Verfahren wegen Strafvereitelung geführt. Zwei Unternehmen hatten je einen Fall wegen Strafvereitelung. Bei einem dieser Unternehmen beruhte dies darauf, dass einige Behörden die Ergebnisse nicht schnell genug bekommen haben. Gegen Mitarbeiter eines Unternehmens liefen im Jahr 2005 drei Verfahren wegen Strafvereitelung.

(8) Drohungen seitens der Behörden

Hinweise seitens der Behörden darauf, dass sich die Mitarbeiter von Telekommunikationsunternehmen bei Weigerung wegen Strafvereitelung strafbar machen bzw. dass sie mit Ordnungs- oder Zwangsmitteln belegt werden können, kommen bei fast allen befragten Unternehmen vor. Ein Befragter führt dazu aus, dass dies häufig im Anschreiben oder im Beschluss stehe. Ein anderer Befragter schildert, dass dies Standard sei bei jeder Zeugenbelehrung bzw. bei jeder Anfrage. Es stehe in der Rechtsbehelfsbelehrung. Zudem würden regelmäßig entsprechende Hinweise durch die Polizei und die Staatsanwaltschaft erfolgen, wenn diese die Ergebnisse dringend benötigen. Wenn es länger dauere (aufgrund erhöhter Anfragen), würden Hinweise auf Strafvereitelung folgen. Auch drei weitere Befragte berichten von regelmäßigen Androhungen von Zwangsmaßnahmen bzw. mit der Einleitung von Strafverfahren wegen Strafvereitelung (z. B. wenn Daten nicht herausgegeben werden können). Dies erfolge meistens telefonisch. Zwei dieser Befragten führen aus, dass das Verhalten – gerade der Staatsanwaltschaft – teilweise an ver-

suchte Nötigung grenze. Einer der Befragten meint, dass immer die Gefahr bestehe, entweder wegen Strafvereitelung belangt zu werden oder weil man die Vorschriften des TKG nicht einhalte (§ 88 TKG, Speicherfristen, etc.).

b) Polizeibeamte

(1) Probleme zwischen Polizei, Staatsanwaltschaft und Gericht

Die befragten Polizeibeamten gaben an, dass es bei der Zusammenarbeit zwischen Polizei, Staatsanwaltschaft und Gericht zu nur wenigen (7) oder keinen (6) Problemen gekommen sei. Probleme kämen nur in Einzelfällen vor. Eine angesprochene Schwierigkeit bezog sich auf die teilweise Unkenntnis der Richter über die Zulässigkeit der Überwachung in die Zukunft. Am Anfang habe der Geschäftsvorgang zwischen Polizei, Staatsanwaltschaft und Gericht zu lange gedauert. Es seien zwei bis vier Wochen vergangen, bis der Beschluss bei der Polizei angekommen sei. Dann habe gerade beim Zielsuchlauf keine Chance mehr bestanden, die Daten zu erlangen. Jetzt bestehe aber ein kurzer Draht zwischen den Beteiligten. Weiteres Problem sei die Fehlerhaftigkeit von Beschlüssen. Die Provider würden sehr auf eine korrekte Form der Beschlüsse achten. Falsche Rufnummern, fehlende Adressaten etc. würden nicht akzeptiert. Dann müsse ein Änderungsbeschluss erlassen werden und es komme zu Verzögerungen. Mit der Staatsanwaltschaft werde die Anregung ausführlich durchgesprochen.

Probleme würden sich dann ergeben, wenn kein Zeuge aussagt, dass die Täter telefoniert haben. Dass Telekommunikation eine Rolle gespielt hat, sei dann schwierig nachzuweisen. Dann könne nur mit Erfahrungswissen argumentiert werden. Bei schwerwiegenden Delikten spiele Telekommunikation unter den Tätern immer eine Rolle. Es erfolgen Absprachen über Mobiltelefone vor und nach der Tat. Diese Aspekte werden dann mit der Staatsanwaltschaft und dem Gericht diskutiert. Allgemein käme es durch unterschiedliche Bewertungen der rechtlichen Voraussetzungen zu Schwierigkeiten. Es gebe auch Meinungsverschiedenheiten über die Notwendigkeit der Maßnahme. Problematisch sei auch die Erreichbarkeit von Richtern gewesen. Ferner gebe es auch technische Probleme. Die Beschlüsse würden den Netzbetreibern nicht zeitnah zugeleitet und auf die Dringlichkeit müsse hingewiesen werden.

(2) Probleme mit den Netzbetreibern

Es wurden verschiedene Probleme bei der Zusammenarbeit mit den Netzbetreibern geschildert. Es gebe interpretationsbedürftige rechtliche Vorgaben. Es sei problematisch, dass die Anbieter die Daten in unterschiedlichen Formaten zu ihnen schicken. Die Daten kämen auf Papier, CD, Diskette oder per Fax. Das mache die Bearbeitung schwieriger. Eine gesetzliche Vorgabe zur Vereinheitlichung der Datenformate wäre wünschenswert (fünf der Befragten). Die Übersendung der Daten in elektronischer Form erleichtere die Auswertung. Die Daten seien für sie nur effektiv verwertbar, wenn sie in digitaler Form geliefert werden. Bei der Lieferung von Listen in Papierform müssten diese eingescannt oder abgeschrieben werden. Dadurch entstünden neben Kosten auch Fehlerquellen. Wegen Fehlens einer gesetzlichen Grundlage würden die Anbieter auf die Bitte um Übersendung in digitaler Form darauf hinweisen, dass sie dazu nicht gesetzlich verpflichtet seien. Selbst auf richterliche Anweisung hin würden sich die Anbieter weigern, berichtet ein Befragter. Eine rechnergestützte Auswertung sei erforderlich, da sonst zu viele Personen beteiligt seien und zuviel Zeit investiert werden müsse. Zudem berichtet ein Befragter von unübersichtlichen Antworten der Netzbetreiber. So würden kommende und abgehende Daten separat und nicht zeitgleich geschickt. Ebenso sei es bei Funkzellenabfragen. Bei acht Funkzellen gebe es acht Antworten pro Unternehmen. Es sei wünschenswert, dass die Antworten schnell und zusammenhängend erfolgen würden.

Ein weiteres Problem sei, dass ein Anbieter keine Daten auf eine Eilanordnung hin herausgebe. Der Netzbetreiber erhebe die Daten daraufhin zwar, gebe sie aber erst nach der Bestätigung durch den Richter heraus. Das widerspreche dem Prinzip der Eilanordnung und den gesetzlichen Vorgaben. Problematisch sei auch, dass es zu lange dauere, bis die Daten geliefert werden. Manche Anbieter würden sich nicht daran halten, dass die Daten unverzüglich geliefert werden müssen, wie es gesetzlich vorgeschrieben ist. Es käme teilweise zu vier bis sechs Wochen Zeitverzug. Dann seien die Daten nicht mehr so relevant. Gerade bei den kleinen Provider (Subprovidern) sei dies eher schwierig. Ein Befragter berichtet, dass man gerade bei Datenabfragen, die in die Zukunft gerichtet sind, immer wieder nachfragen müsse. Sie hätten aber keine Handhabe, um die Netzbetreiber zu verpflichten, die Daten zeitnah zu liefern. Ein Anbieter berichtet, dass die Richter mittlerweile auch anordnen, bis wann die Daten geliefert werden müssen. Folgemaßnahme bei Nichtlieferung sei dann die Durchsuchung und Sicherstellung der Daten bei den Betreibern.

Schwierigkeiten bereite auch die Erreichbarkeit der Netzbetreiber. Sie seien nur zu ihren Bürozeiten erreichbar und nicht am Wochenende, zu Nachtzeiten oder an Feiertagen. Kriminalität fände aber rund um die Uhr statt. Das sei problematisch, da es bei eiligen Sachen und schwerer Kriminalität zu Datenverlust kommen könne. Aber dies sei nicht gesetzlich festgelegt. Die Netzbetreiber würden sehr viel Wert auf formale Kriterien legen und hielten diese penibel ein. Die Anbieter hätten teilweise eine eigene Rechtseinschätzung und würden Beschlüsse anzweifeln. Zu Problemen käme es auch immer dann, wenn es zu einer Umstellung aus datenschutzrechtlicher Sicht käme.

Grundsätzlich habe eine deutliche Verbesserung in den letzten Jahren stattgefunden. Man arbeite regelmäßig zusammen und Probleme könnten telefonisch geklärt werden. Es gebe geringe Reibungspunkte. Die Provider würden sich nach Kräften bemühen. Weiter wurde angegeben, dass dies unterschiedlich und vor allem firmen- und personenabhängig sei. Manche Mitarbeiter der Unternehmen seien sehr kooperativ, andere würden sich

völlig querstellen. Teilweise erfolge keine Prioritätensetzung bei herausragenden Fällen. Bei manchen Anbietern ginge es schnell, bei manchen seien die Daten unvollständig oder unleserlich gemacht. Die anonymisierten Daten seien zum Beweis unbrauchbar.

(3) Speicherprobleme

Fälle, bei denen der Zugriff auf Verkehrsdaten notwendig gewesen wäre, dem Auskunftsersuchen aber nicht (ausreichend) nachgekommen werden konnte, da die Daten bei den Anbietern bereits gelöscht waren oder nur teilanonymisiert gespeichert, sind den meisten der Befragten bekannt. Das, so heißt es, komme häufiger vor. Da es keine gesetzliche Regelung zur Speicherdauer gibt, richtet sich diese nach der mit dem Kunden geschlossenen Vereinbarung. Die Daten würden zwischen drei und 180 Tagen gespeichert. Nach einem Befragten wären Meldung und Sammlung der Fälle wichtig, um eine Problembeseitigung einzuleiten. Ein Befragter ist der Ansicht, dass es nicht immer an den Providern liege, dass die Daten schon gelöscht seien. Manchmal dauere die Antragstellung einfach zu lange. Ein Befragter schilderte, dass die Speicherfristen bei ausländischen Rufnummern Schwierigkeiten bereiten würden (30-Tages-Frist). Internetanbieter würden IP-Adressen teilweise überhaupt nicht speichern.

Einer der Befragten erklärte, dass der Entwurf zur Novellierung der verdeckten Ermittlungsmaßnahmen eine zu lange Einführungszeit habe (erst ab 2009), insbesondere, was Internetspuren betreffe. Ebenso sei unverständlich, dass die großen Anbieter bis 2009 ihre bisherigen Speicherfristen reduzieren wollen. Zumindest die bisherigen Speicherfristen sollten beibehalten werden und ab 2009 dann die veränderten Speicherfristen umgesetzt werden. Straftaten im Umgang mit den neuen Medien seien sonst nicht mehr aufklärbar.

(4) Verschlüsselungstechniken

Mit Verschlüsselungstechniken der Täter hatten sechs der befragten Polizeibeamten Probleme. Es wurde erläutert, dass durch Anonymisierungsdienste im Internet ein rechtsfreier Raum entstehe. Durch Anonymisierungsmethoden würden die Spuren der Täter verwischt. Dann bestünde die Gefahr, dass andere Personen als der Täter ins Visier der Ermittlungen gelangen. Insbesondere beim sog. „Phishing“ sei dies verbreitet: Danach würden IP-Adressen bei Bankrechnern gespeichert. Wenn diese rückverfolgt würden, führe die Spur nicht zu den Tätern, sondern zu Rechnern, die mit Trojanern verseucht seien. Angegeben wurde auch, dass Anonymisierungsdienste bisher nur im Bereich Internet, aber nicht bei der Telefonie angewandt würden. Bei letzterer seien Probleme bislang nur im Zusammenhang mit § 100a StPO vorgekommen. Ein Befragter gab an, dass Verschlüsselungstechniken nur in etwa jedem zehnten Fall vorkämen. Ein anderer meinte, dass die Nutzung von Verschlüsselungstechniken zunehme. Ein Befragter gab an, dass die Täter die Verschlüsselung dadurch versuchen, indem Spuren über Mailboxen und Weiterleitungen verwischt würden. Dies gelinge allerdings deshalb nicht, weil diese Wege verfolgt werden könnten. Zudem seien Voice over IP und dynamische IP-Adressen ein Problem. Es sei unklar, wer mit wem kommuniziert habe. Von den Anbietern werde nicht geprüft, welche Person sich freischalten lässt.

c) Staatsanwälte

(1) Probleme zwischen Polizei, Staatsanwaltschaft und Gericht

Etwa die Hälfte der befragten Staatsanwälte gab an, dass es keine Probleme bei der Zusammenarbeit mit der Polizei und dem Gericht gebe. Im Übrigen wurde ausgeführt, dass im Einzelfall unterschiedliche Auffassungen zwischen den Beteiligten bestehen würden. Die Polizei rege etwas an, was die Staatsanwaltschaft nicht für erforderlich halte. Ebenso sei auch ab und zu das Ermittlungsgericht anderer Auffassung, z. B. was die Erheblichkeit einer Straftat angehe oder die Verhältnismäßigkeit. Problematisch sei, der Polizei zu vermitteln, dass die Voraussetzungen nicht vorliegen. Die Polizei kenne die rechtlichen und technischen Voraussetzungen oftmals nicht. Das sei ein Problem der Fortbildung. Dazu wurde ausgeführt, dass es bei der Funkzellenabfrage Probleme mit der Polizei gegeben habe. Diese sei extrem oft beantragt worden. Es bedürfe jedoch tatsächlicher Anhaltspunkte, dass überhaupt telefoniert worden sei. Problematisch sei früher die örtliche Zuständigkeit des Gerichts gewesen. Umstritten war, ob das Gericht am Sitz des Unternehmens oder am Sitz der Zweigstelle, bei der die Daten gespeichert würden, zuständig sei. Diesbezüglich sei aber eine Klarstellung durch den Bundesgerichtshof erfolgt.

(2) Probleme mit den Netzbetreibern

Mit den Netzbetreibern seien keine Schwierigkeiten aufgetreten, geben vier befragte Staatsanwälte an. Einer von ihnen erläutert dazu, dass es früher Probleme gegeben habe, mittlerweile aber nicht mehr. Weiteres Problem sei die Weigerung der Datenherausgabe – selbst mit Beschluss. Manche Anbieter würden kooperieren, manche nicht. Manche würden „nur auf Druck reagieren“. Die Staatsanwaltschaft drohe in Fällen, in denen die Anbieter die Daten selbst auf einen Beschluss hin nicht herausgeben, mit einem Verfahren wegen Strafvereitelung. Des Weiteren gebe es Anbieter, die sich weigern würden, die Daten zu sichern. Eilanordnungen durch die Staatsanwaltschaften würden sich problematisch gestalten. Weiter wurde ausgeführt, dass das Antwortverhalten nicht zufrieden stellend sei. Die Beantwortung sei zum Teil äußerst zögerlich erfolgt und in manchen Fällen (z. B. Bankraub) sei es aus ihrer Sicht einfach unabdingbar, dass die Auskunft schnell erfolge. Sie hätten nicht das Gefühl, dass die Provider mit großem Einsatz hinter den Ermittlungen stehen.

Zudem werde von einem Anbieter für Bestandsdaten ein Beschluss nach §§ 100g, 100h StPO verlangt, bei dem aber eigentlich § 113 TKG einschlägig sei. Begründet werde dies damit, dass sie VerbindungsdatenVerkehrsda-

ten abfragen müssen, um an die Bestandsdaten zu kommen. Dies sei jedoch Angelegenheit der Provider. In solchen Fällen würden Drohschreiben aufgesetzt.

Weiteres Problem, das angeführt wurde, bezieht sich auf die unterschiedlichen Speicherfristen der Anbieter. Eine einheitliche Speicherungsdauer sei sinnvoll. Kritisiert wird auch, dass die Wochenendbereitschaft der Anbieter fehle. Zudem seien die Premiumrate (0190)-Nummern der Netzbetreiber problematisch. Für §§ 100a, 100b StPO sei dies verboten, für §§ 100g, 100h StPO dagegen nicht. Teilweise gaben die Befragten an, dass sie die Probleme nur mittelbar über Informationen der Polizei verfolgen können.

(3) Speicherprobleme

Fälle, in denen der Zugriff auf Verkehrsdaten notwendig gewesen wäre, die Daten aber bereits gelöscht oder nur teilanonymisiert gespeichert waren, gibt es nach Angabe der Hälfte der befragten Staatsanwälte häufig. Das liege daran, dass die Straftat erst später bekannt werde. Dann könne die Maßnahme nicht mehr durchgeführt werden. Zum Teil würden auch die Geschädigten die Straftat zu spät anzeigen. Drei Befragte meinen, es sei vorgekommen, dass die Daten zu kurz gespeichert waren. Drei weiteren Befragten sind keine solchen Fälle bekannt. Ein Befragter meint, dass es eher die Ausnahme sei, dass es Probleme mit den Speicherfristen gebe. Die Maßnahme werde sehr häufig in die Zukunft angeordnet bzw. aktuelle Daten seien wichtiger. Ein weiteres Problem seien auch die Fälle, in denen der Sitz des Servers im Ausland sei.

(4) Verschlüsselungstechniken

Ob die Befragten mit Verschlüsselungstechniken der Täter in Berührung gekommen sind, beantworten vier der Staatsanwälte mit nein. Ein Befragter meinte, Skype stelle ein Problem dar. Das könnten sie nicht abhören. Ein Befragter aus einem Dezernat, das Computerkriminalität behandelt, gibt an, dass es Verschlüsselungstechniken durch Verwendung von Proxyservern gebe. Dann führe die ermittelte IP-Adresse nicht zum Ergebnis. Die Handlungen seien von einem anderen PC ausgeübt worden. Das sei sehr häufig

d) Richter

(1) Probleme zwischen Polizei, Staatsanwaltschaft und Gericht

Über die Hälfte der Befragten berichteten, dass es (grundsätzlich) zu keinen Problemen bei der Zusammenarbeit mit der Polizei und der Staatsanwaltschaft im Rahmen der Verkehrsdatenabfrage gekommen sei. Wenn es Probleme gebe, würden diese telefonisch besprochen und geklärt. Ein Problem sei, dass (selten) keine ausreichende Begründung dafür gegeben würde, warum eine bestimmte Nummer beteiligt sein solle. Die Anträge seien dann zurückgenommen worden. Weitere angegebene Probleme seien Zahlendreher bei den Rufnummern und sonstige Fehler. Der Beschluss müsse dann berichtigt werden. Die Polizei stelle Verlängerungsanträge teilweise zu spät. Zudem finde keine Benachrichtigung über die Abschaltung einer Telefonüberwachung statt, obwohl dies gesetzlich vorgesehen sei. Weiter wurde berichtet, dass es Probleme zwischen der Polizei und der Staatsanwaltschaft gebe. Die Polizei beantrage die Maßnahme gerne und die Staatsanwaltschaft lehne die Anträge des Öfteren ab. Die Polizei müsse da „gebremst“ werden.

(2) Probleme mit den Netzbetreibern

Es wurde berichtet, dass es mit den Netzbetreibern Probleme wegen der Datenspeicherung gebe. Die Daten würden nur drei Monate gespeichert. Manchmal sei es dann zu spät. Die unterschiedlichen Speicherungsmodalitäten bei den Anbietern seien problematisch. Einige Anbieter würden den Beschluss nicht nur per Fax haben wollen, sondern im Original und mit Siegel. Ein Richter meint, wenn der Anbieter die Maßnahme sonst nicht durchführe, grenze dies an Strafvereitelung. Seiner Meinung nach hätten die Anbieter keinen Anspruch auf den Originalbeschluss. Die Anbieter würden sehr auf Formalitäten achten. Das sei aber auch in Ordnung, äußerte ein anderer Richter. Ein Befragter hat den Eindruck, dass die Anbieter alle Anfragen umsetzen, wenn ein Beschluss vorhanden sei. Sie hätten Sorge, etwas falsch zumachen. Teilweise erfolge eine zögerliche Umsetzung der Beschlüsse. Die Anbieter würden sich teilweise weigern, die Maßnahmen durchzuführen, obwohl ein Beschluss vorläge. Die Anbieter seien der Ansicht, dass sie die Beschlüsse überprüfen müssten. Das sei aber nicht ihre Aufgabe, sondern die des Landgerichts. Sie würden sich als „Hüter der Verfassung“ aufspielen, obwohl ihre Aufgabe nur in der Umsetzung der Beschlüsse bestünde. Es sei aber auch vorgekommen, dass Anbieter Verkehrsdaten auf CD schickten ohne Angabe eines Aktenzeichens und ohne Anschreiben. Es mache den Anschein, als seien sich die Anbieter manchmal nicht über die Brisanz der Daten bewusst.

Problematisch sei die Auskunft zu dynamischen IP-Adressen. Es gebe immer wieder Diskussionen darüber, ob ein Beschluss dafür notwendig sei oder nicht. Es sei aber mehrfach entschieden worden, dass §§ 100g, 100h StPO nicht einschlägig seien. Trotzdem würden die Anbieter auf einem Beschluss beharren. Dann müsse in jedem Fall neu darüber entschieden werden.

Probleme gebe es in Bezug darauf, ob eine Eilanordnung innerhalb von drei Tagen bestätigt werden muss. Einer der befragten Ermittlungsrichter gibt an, dass sie der Meinung sind, dass die Staatsanwaltschaft die Maßnahme für drei Tage anordnen dürfe und nur, wenn sie Daten über diese 3 Tage hinaus brauchen, dann müsse eine richterliche Bestätigung erfolgen. Die Anbieter würden jedoch die Auffassung vertreten, dass die Staatsanwaltschaft für diese drei Tage eine Bestätigung benötige. Ohne die Bestätigung würden sie die Daten nicht herausgeben. Dagegen seien sie machtlos und daher würden sie, um die Ermittlungen nicht zu behindern, die richterlichen Bestä-

tigungsbeschlüsse erlassen, obwohl sie der Meinung seien, dass sie gar nicht notwendig seien.

(3) Speicherprobleme

Der Hälfte der Befragten sind keine Fälle bekannt, in denen der Zugriff auf Verkehrsdaten notwendig gewesen wäre, die Daten aber bereits gelöscht oder nur teilanonymisiert gespeichert waren. Ein Richter gibt an, dass er eilige Anfragen bekomme, die am Ende der Frist liegen. Die Staatsanwaltschaft sei aber genau über die Speicherfristen informiert. Zwei andere Befragte führten aus, dass sie von der Auswertung und der Durchführung der Maßnahmen keine Kenntnis haben (nur wenn die Akte wiederkommt). Im Übrigen wurde angegeben, dass solche Fälle vorkommen. Die gesetzlichen Fristen seien abgelaufen gewesen, was aber kein Verschulden der Netzbetreiber sei. Ein Anbieter lösche die Daten verfrüht (teilweise Speicherung nur noch für einen Monat). Andererseits sei unklar, was für Datenmengen die Anbieter zu bewältigen haben. Ein anderer Befragter findet, dass eingehende Anrufe länger als 72 Stunden gespeichert werden sollten. Diese Frist sei zu kurz. Wahrscheinlich würden viele Maßnahmen durchgeführt, obwohl es gar nicht nötig gewesen sei, nur weil die Ermittler wüssten, dass die Daten nach den 72 Stunden nie wieder zu beschaffen seien. Zudem erfolge die Speicherung bei den Anbietern uneinheitlich. Eine Vereinheitlichung sei sinnvoll. Problematisch seien die Speicherfristen (bei den ausländischen Unternehmen) auch, wenn Mobiltelefone aus dem Ausland benutzt würden, was beim Enkeltrick verbreitet sei. Ein Befragter schilderte, dass vor allem bei Internetkriminalität Probleme auftauchen würden. Es würden Dienste in Anspruch genommen werden, die nicht bezahlt würden. Da es jedoch um nicht so große Schäden handle, würden diese Fälle nachrangig behandelt. Die Daten seien dann nicht mehr vorhanden. Mit teilanonymisierten Daten habe er bisher keine Fälle gehabt, meint ein Befragter.

e) Verteidiger

Dass Daten, die für den Mandanten eine entlastende Wirkung gehabt hätten, bereits gelöscht waren oder nur noch teilanonymisiert gespeichert waren, kam nur bei einem der befragten Verteidiger vor. Man müsse den Zugriff in einem frühen Stadium des Verfahrens beantragen, damit die Löschung der Daten verhindert werde.

4. Zusammenfassung der Ergebnisse

Die technische Umsetzung der Verkehrsdatenabfrage erfolgt durch die Telekommunikationsanbieter. Nachdem die Anfrage bei Ihnen eingeht, wird überprüft, um welche Art von Abfrage es sich handelt und ob die formellen Voraussetzungen gegeben sind. Die Hälfte der Netzbetreiber sieht sich – entgegen der Ansicht der Polizei- und Justizbehörden – dazu verpflichtet, darüber hinaus auch materielle Erwägungen anzustellen. Beschwerden wegen von ihnen monierter Unverhältnismäßigkeit der Verkehrsdatenabfrage, z. B. wegen Geringfügigkeit des Anlassdelikts, bleiben erfolglos. Der Suchlauf wird von den jeweiligen Sachbearbeitern gestartet und elektronisch oder in Papierform zu den anfragenden Stellen geschickt. Bei der Durchführung der Maßnahmen sind zwischen den Beteiligten verschiedene Schwierigkeiten aufgetreten. Die Zusammenarbeit zwischen Polizei, Staatsanwaltschaft und Gericht wird überwiegend als gut bewertet. Dies ergibt sich sowohl aus der schriftlichen Befragung, bei der die befragten Staatsanwälte die Zusammenarbeit als gut bis sehr gut (94 Prozent) bezeichneten, als auch aus den Experteninterviews mit Polizeibeamten, Staatsanwälten und Richtern. In den Gesprächen führten die Beteiligten an, dass es teilweise Meinungsverschiedenheiten hinsichtlich der rechtlichen Bewertungen und der Notwendigkeit der Maßnahme geben würde. Staatsanwälte und Richter äußerten zudem, dass die Polizei teilweise die rechtlichen Voraussetzungen nicht kenne und Maßnahmen (z. B. Funkzellenabfragen) anrege, obwohl keine Anhaltspunkte dafür vorlägen, dass telefoniert worden ist. Es würde nicht immer ausreichend begründet, warum ein bestimmter Anschluss beteiligt sein soll. Weitere Probleme betreffen fehlerhafte Rufnummern. Probleme mit den Netzbetreibern werden hingegen häufig genannt. Die Zusammenarbeit wird zwar nach den Ergebnissen der schriftlichen Befragung überwiegend als mittelmäßig bis gut empfunden. Es wurden jedoch gelegentliche bis häufige Schwierigkeiten durch Verzögerungen bzw. zu kurze Speicherungszeiträume angegeben. Gelegentlich seien Anordnungen nicht akzeptiert worden. Dies wird auch durch die Ergebnisse der Aktenanalyse bestätigt. Allerdings konnte dies nur bei 27 von 1 257 Beschlüssen den Akten entnommen werden. Zu einem großen Teil beruhte dies auf der Nichtakzeptierung von Eilanordnungen ohne richterliche Bestätigung. Im Übrigen handelte es sich jedoch um fehlerhafte Beschlüsse, die falsche oder unvollständige Rufnummern enthielten, oder sonstige nicht im Verantwortungsbereich der Anbieter liegende Ausführungshindernisse. Zu Verzögerungen führte das Warten auf die richterliche Bestätigung in sieben Fällen. Weitere Verzögerungen ohne explizite, den Akten zu entnehmende Weigerung der Anbieter kamen bei 32 Beschlüssen vor. Auch hier ging es u. a. um fehlerhafte Beschlüsse, bei denen Rufnummern falsch waren oder kein Abfragezeitraum festgelegt war. In der Sphäre der Anbieter liegende Verzögerungen kamen lediglich in fünf Fällen vor, in denen falsche Daten abgefragt wurden oder die Anfrage wegen Personalmangel nicht erfolgte. Eine weitere Schwierigkeit, die sich aus der schriftlichen und mündlichen Befragung ergibt, ist die nicht vorhandene Wochenendbereitschaft der Anbieter. Den Anbietern wird teilweise mangelnde Kooperationsbereitschaft und Desinteresse an der Zusammenarbeit mit den Strafverfolgungsbehörden vorgeworfen. Aufgrund unklarer Rechtslage gibt es unterschiedliche Rechtsauffassungen. Durch diese Probleme ist es nach den Ergebnissen der schriftlichen Befragung häufig zur Erfolglosigkeit des Auskunftsersuchens und Verfahrensverzögerungen gekommen. In den Expertengesprächen wurde angesprochen, dass die Zusendung der Daten in unterschiedlichen Formaten sowie die nicht unverzügliche Zusendung der Daten proble-

matisch sei. Zudem widerspreche die Weigerung einiger Anbieter, ohne richterliche Bestätigung auf eine Eilanordnung hin die Daten herauszugeben, dem Prinzip der Eilanordnung. Die Anbieter würden zudem sehr auf Formalien achten. Weiteres Problem sei die Forderung eines Beschlusses bei Abfrage von Personendaten zu dynamischen IP-Adressen. Hier ist nach Ansicht der befragten Staatsanwälte und Richter § 113 TKG und nicht die §§ 100g, 100h StPO einschlägig.

Weitere Probleme ergeben sich nach den Ergebnissen der schriftlichen Befragung und der Expertengespräche aus den unterschiedlichen Speicherdauern und daraus, dass Daten zu früh gelöscht werden. Die meisten schriftlich befragten Staatsanwälte (48 Prozent) würden eine Speicherdauer von sechs bis zu zwölf Monaten befürworten. Teilweise wird den Anbietern durch die befragten Praktiker zugestanden, dass es nicht immer an diesen liege, wenn die Daten bereits gelöscht seien, sondern dass die Antragstellung zu spät komme oder die Straftat zu spät bekannt werde. Schwierigkeiten bei der Speicherung der Daten tauchten in den Akten nur bei 63 Beschlüssen auf. Bei 37 Beschlüssen waren die Daten zum Zeitpunkt der Abfrage bereits gelöscht, bei 17 Beschlüssen nur teilanonymisiert gespeichert und bei neun Beschlüssen waren die Daten von vornherein nicht gespeichert. Teilweise konnte den Akten eine Erfolgsbeeinflussung durch diese Faktoren entnommen werden. Dies betrifft vor allem die Anschlüsse, bei denen die Daten bereits gelöscht waren. Schwierigkeiten durch Verschlüsselungstechniken sind nach Angaben der schriftlich und mündlich Befragten kaum vorgekommen. Etwa 70 Prozent der Staatsanwälte, die an der schriftlichen Befragung teilgenommen haben, gaben an, dass diese in ihrer Praxis nie eine Rolle gespielt hätten. Über 50 Prozent konnten keine Auswirkungen angewandter Verschlüsselungstechniken bemerken. Im Rahmen der Expertengespräche gaben Polizeibeamte und Staatsanwälte an, dass Verschlüsselungstechniken vor allem im Internetbereich angewandt wurden. Bei Rückverfolgung der Daten gelange man dann nicht zum Täter, sondern zu unbeteiligten Rechnern. Auch bei der Auswertung der Akten konnte nur ein Fall festgestellt werden, bei dem die Daten verschlüsselt waren, wobei die Auswirkungen auf den Erfolg nicht manifest werden.

Technische Schwierigkeiten waren ebenfalls selten. Nach den Ergebnissen der schriftlichen Befragung erfolgten Beeinträchtigungen dadurch nie (55 Prozent) oder selten (29 Prozent). Als technische Probleme wurden die Löschung von Daten und sonstige Speicherprobleme angegeben. Nur wenige gaben Serverabstürze bei den Providern, Datenverlust und Übermittlungsfehler an. Erfolgsbeeinträchtigungen gab es dadurch nach Angabe von 40 Prozent der Befragten nicht. Ansonsten wurden vor allem Verfahrensverzögerungen und Erfolglosigkeit der Maßnahmen genannt. Aus den Akten waren nur drei Fälle ersichtlich, in denen es technische Probleme gab. In zwei Fällen davon war den Anbietern die Ausführung der Abfrage prinzipiell technisch nicht möglich.

Die Telekommunikationsanbieter schilderten ebenfalls mehrere Schwierigkeiten mit den Polizei- und Justizbehörden. Es wurde technische und rechtliche Unkenntnis genannt, z. B. auch, was die Durchführung von Zielwahlsuchen betreffe. Zudem seien die Beschlüsse oft undeutlich und schwer zu verstehen. Sie seien zu unpräzise und müssten interpretiert werden. Angesprochen wurde auch die Problematik der fehlenden richterlichen Bestätigung bei Eilanordnungen. Weiter wurde angeführt, dass die Praxis zur Auskunft über Personendaten zu dynamischen IP-Adressen uneinheitlich sei. Hierzu gebe es unterschiedliche Rechtsauffassungen und Rechtsprechung. Teilweise fordern die Anbieter dafür einen Beschluss nach §§ 100g, 100h StPO. Geweigert hätten sie sich aber im Jahr 2005 nicht. Beschwerden wurden vereinzelt eingelegt. Nur ein Unternehmen wurde 2005 mit Ordnungs- und Zwangsmitteln belegt, während gegen drei Mitarbeiter eines Unternehmens Verfahren wegen Strafvereitelung geführt wurden. Drohungen seitens der Polizei- und Justizbehörden mit Ordnungs- und Zwangsmitteln sowie mit Einleitung von Strafverfahren wegen Strafvereitelung kommen bei fast allen Telekommunikationsanbietern regelmäßig vor.

VII. Betroffene und Benachrichtigung

Wie viele Betroffene es durchschnittlich bei der Verkehrsdatenabfrage gibt und wie oft die Betroffenen benachrichtigt werden, ist Gegenstand des folgenden Abschnitts.

1. Schriftliche Befragung

a) Benachrichtigung der Betroffenen

Die Schätzung der Anzahl der zu benachrichtigenden Betroffenen durch die schriftlich Befragten ergab eine relativ breite Verteilung. So nannten 34 Prozent der Befragten einen Betroffenen, der zu benachrichtigen ist, 28 Prozent zwei, 22 Prozent drei bis fünf, 6 Prozent sechs bis zehn und 9 Prozent mehr als zehn Betroffene. Damit wurden im Durchschnitt ca. 3,5 zu benachrichtigende Betroffene pro Maßnahme genannt. Der Anteil nicht benachrichtigter Betroffener wurde im Mittel auf 38 Prozent geschätzt, wobei dieser Wert je nach in der vorausgegangenen Frage angegeben Personenzahl deutlich differierte. So steigt die Quote der Nichtbenachrichtigten von etwa 31 Prozent (wenn nur eine Person betroffen war) auf ca. 64 Prozent, wenn mehr als zehn Personen betroffen waren. Ähnlich verhält es sich bei der Zurückstellung der Benachrichtigung aus Gründen des § 101 I StPO. Hier wurde im Mittel ein Anteil von 35 Prozent geschätzt. Dieser Wert nimmt gleichfalls mit der Anzahl der Betroffenen von 29 Prozent (ein Betroffener) auf 46 Prozent (mehr als zehn Betroffene) zu.

Etwa die Hälfte aller Befragten nannte explizit Gründe für die Nichtbenachrichtigung oder Zurückstellung einer Benachrichtigung. Von diesen gaben 29 Prozent die Gefährdung des Untersuchungszwecks, des Ermittlungserfolges bzw. weiterer Ermittlungen, z. B. auch in anderen laufenden Verfahren, an. In die gleiche Richtung

geht die Begründung derjenigen, die auf „Ermittlungstaktik“ verwiesen (10 Prozent). Ca. 13 Prozent führten an, dass der hohe Aufwand der Grund für die Nichtbenachrichtigung sei und 6 Prozent gaben Arbeitsüberlastung an. Weiter wurde begründet, dass die Teilnehmer bzw. Anschlussinhaber meist gar nicht identifiziert würden (10 Prozent) und die Betroffenen extra zur Benachrichtigung ermittelt werden müssten, was (auch gegenüber den Betroffenen) unverhältnismäßig und mit hohem Aufwand verbunden sei (5 Prozent). 8 Prozent räumten ein, dass die Nichtbenachrichtigung auf Vergesslichkeit beruhe und weitere 10 Prozent auf Nachlässigkeit, Versehen und Übersehen. Ein weiterer Grund für die Nichtbenachrichtigung sei, dass der Beschuldigten durch das Verfahren bzw. durch Akteneinsicht ohnehin von der Maßnahme erfahre und es daher keiner Benachrichtigung bedürfe (5 Prozent). 4 Prozent meinten, die Nichtbenachrichtigung beruhe oftmals darauf, dass V-Leute und Zeugen geschützt werden sollten. Weitere Begründungen waren, dass es eine Vielzahl an Betroffenen gebe, dass der Täter bzw. seine Adresse unbekannt sei, dass die Nichtbenachrichtigung zur Vermeidung von Verunsicherung der Betroffenen erfolge und dass die Benachrichtigung aller Betroffenen unpraktikabel sei und hohe Kosten verursache.

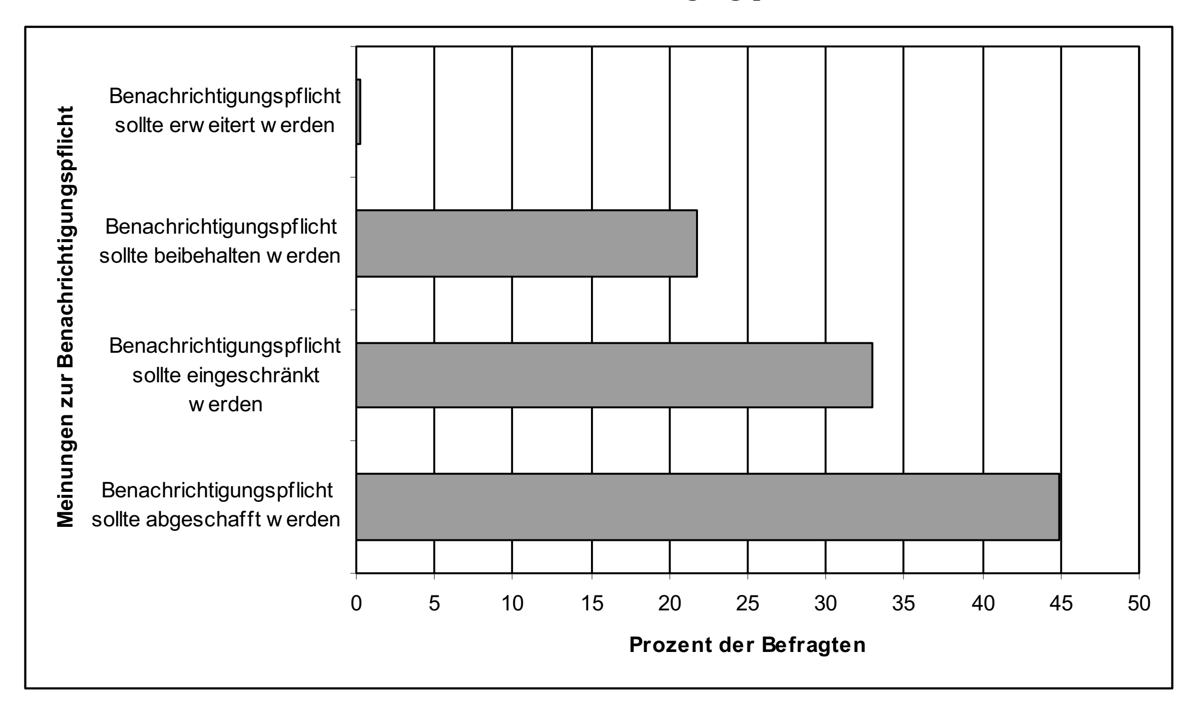
b) Beurteilung der Benachrichtigungspflicht

Ob die Benachrichtigungspflicht unverändert beibehalten werden sollte, beantworteten die Befragten unterschiedlich.

22 Prozent sprachen sich für die Beibehaltung der Benachrichtigungspflicht aus (siehe Abbildung 78). Die Mehrheit der Befragten wollte sie eingeschränkt (33 Prozent) oder ganz abgeschafft (45 Prozent) haben. Nur zwei Befragte befürworteten eine Erweiterung der Benachrichtigungspflicht.

Abbildung 78

Ansichten zur Benachrichtigungspflicht



2. Aktenanalyse

Bei der Auswertung der Verfahrensakten wurde erfasst, wie viele Personen von den Verkehrsdatenabfragen betroffen waren.

a) Betroffene der Verkehrsdatenabfrage

Unmittelbar betroffen von den Maßnahmen sind die Personen, deren Anschlüsse direkt durch die Maßnahmen nach §§ 100g, 100h StPO abgefragt wurden. Dies sind die Anschlussinhaber, ggf. weitere Inhaber des Anschlusses (z. B. bei Ehepaar/Familie) und die Nutzer der Anschlüsse. Darüber hinaus sind zumindest mittelbar alle Anschlüsse betroffen, die bei der Abfrage des überwachten Anschlusses mit abgefragt wurden. Diese Zahl der Anschlüsse konnte von uns nicht bestimmt werden. Die Massen an Daten, die bei einer Funkzellenabfrage oder einer Zielwahlsuche entstehen, sind nicht zählbar. Außerdem sind zwei weitere Aspekte zu berücksichtigen: Zum einen befanden sich die Daten teilweise auf einer CD-Rom und in den Akten war nur ein Ausschnitt davon erfasst. Zum anderen kamen auf den Datenauszügen Anschlussnummern teilweise mehrfach vor und es war nicht ersichtlich, welche Rufnummer zu welchem Anschlussinhaber gehört. Das heißt, es könnten mehrere aufgeführte Rufnummern zu einem Anschlussinhaber gehören (z. B. ISDN oder wenn derjenige ein Festnetztelefon und ein Handy besitzt). Im Folgenden sind also nur die Betroffenen aufgeführt, deren Anschlüsse unmittelbar überprüft wurden und ggf. weitere Inhaber dieser Anschlüsse. Es gibt 1 645 unmittelbar betroffene Anschlussinhaber, die identifiziert werden konnten. Davon sind 505 Beschuldigte und 1 110 Dritte. Bei den übrigen identifizierten Anschussinhabern sind sowohl der Beschuldigte als auch ein Dritter Anschlussinhaber. Wie sich Beschuldigte und Dritte als Anschlussinhaber prozentual auf die Anschlüsse verteilen, lässt sich Abbildung 79 entnehmen.

Die Nutzer konnten bei 1 709 Anschlüssen identifiziert werden. Die überprüften Anschlüsse wurden nicht immer von den Inhabern selbst benutzt. So war der Beschuldigte nur in etwa 30 Prozent der Fälle der Anschlussinhaber, aber in über 40 Prozent der Fälle alleiniger Nutzer des Anschlusses (siehe Abbildung 80). Diejenigen Anschlüsse, deren Inhaber Dritte waren, wurden in 22 Prozent der Fälle vom Beschuldigten genutzt. 60 Prozent dieser Anschlüsse wurden nur von dem Dritten und 19 Prozent von Beschuldigtem und Drittem genutzt.

In Abbildung 81 wird dargestellt, in welchem Verhältnis der Anschlussinhaber zum Beschuldigten stand, wenn es sich bei dem Inhaber um eine Dritten handelte. Dies konnte nur bei etwa der Hälfte der Anschlüsse festgestellt werden. Meist handelte es sich bei dem Inhaber des Anschlusses um das angerufene Opfer der Straftat oder um Personen aus dem Umfeld des Opfers (39 Prozent). Häufig handelte es sich bei den überwachten Anschlüssen auch um Rufnummern der Familie des Beschuldigten (18 Prozent). Keine Beziehung von Beschuldigtem und Anschlussinhaber war bei 15 Prozent festzustellen und bei 5 Prozent war der Anschlussinhaber unbekannt. Um Kontaktpersonen handelte es sich bei 6 Prozent und um Szenebekanntschaften bei 5 Prozent der Inhaber. Freunde und Bekannte des Beschuldigten waren zu 4 Prozent betroffen.

Abbildung 79



Inhaber der überwachten Anschlüsse

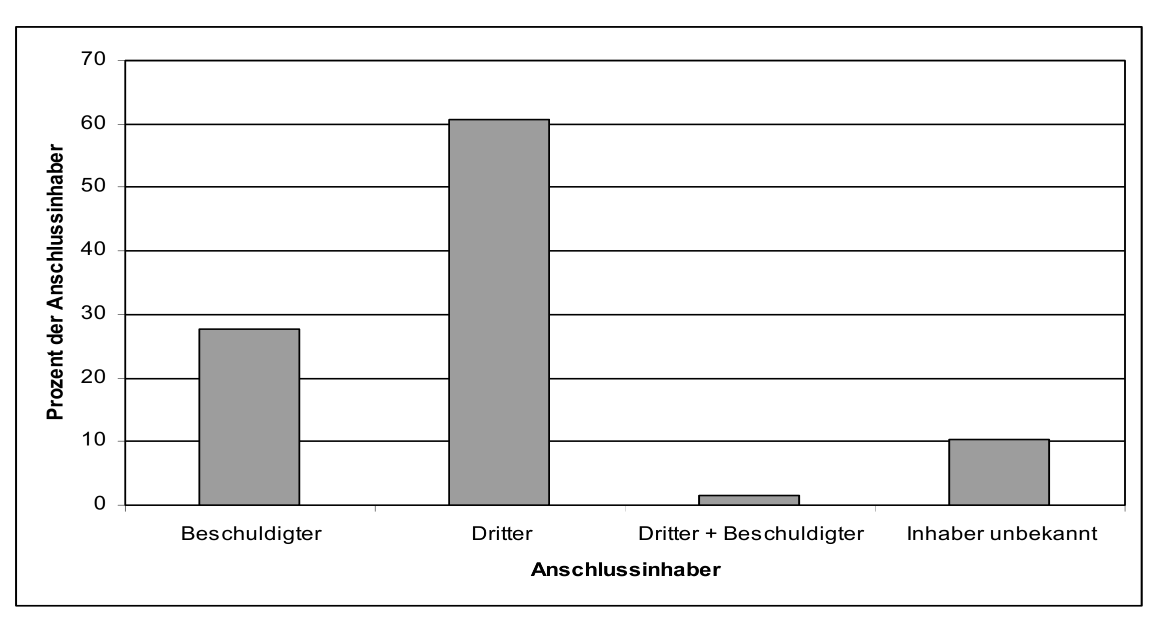


Abbildung 80



Nutzung der Anschlüsse

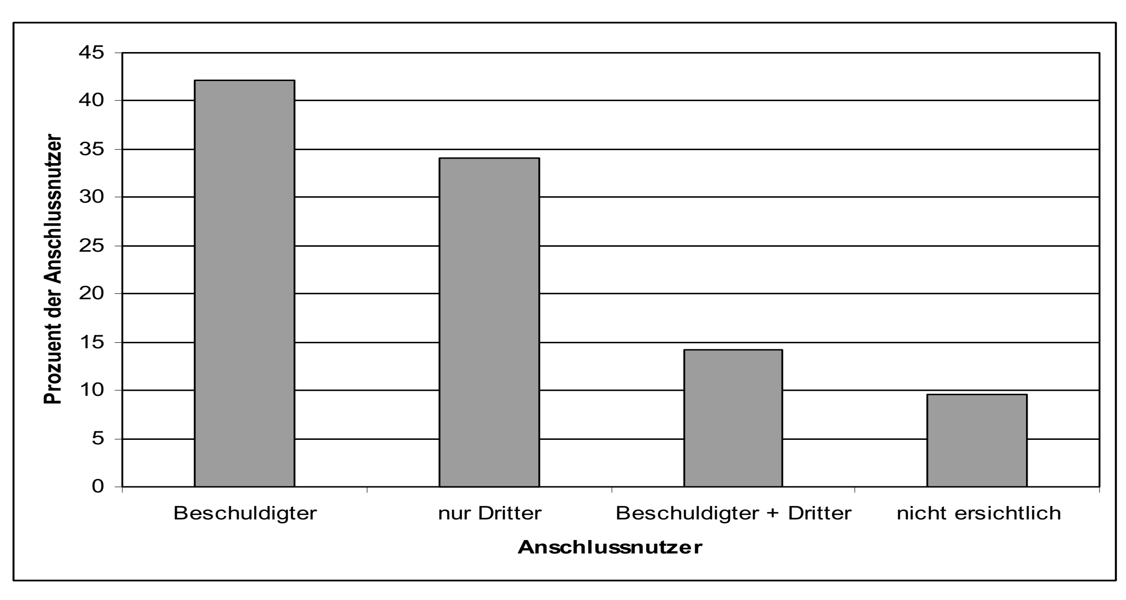
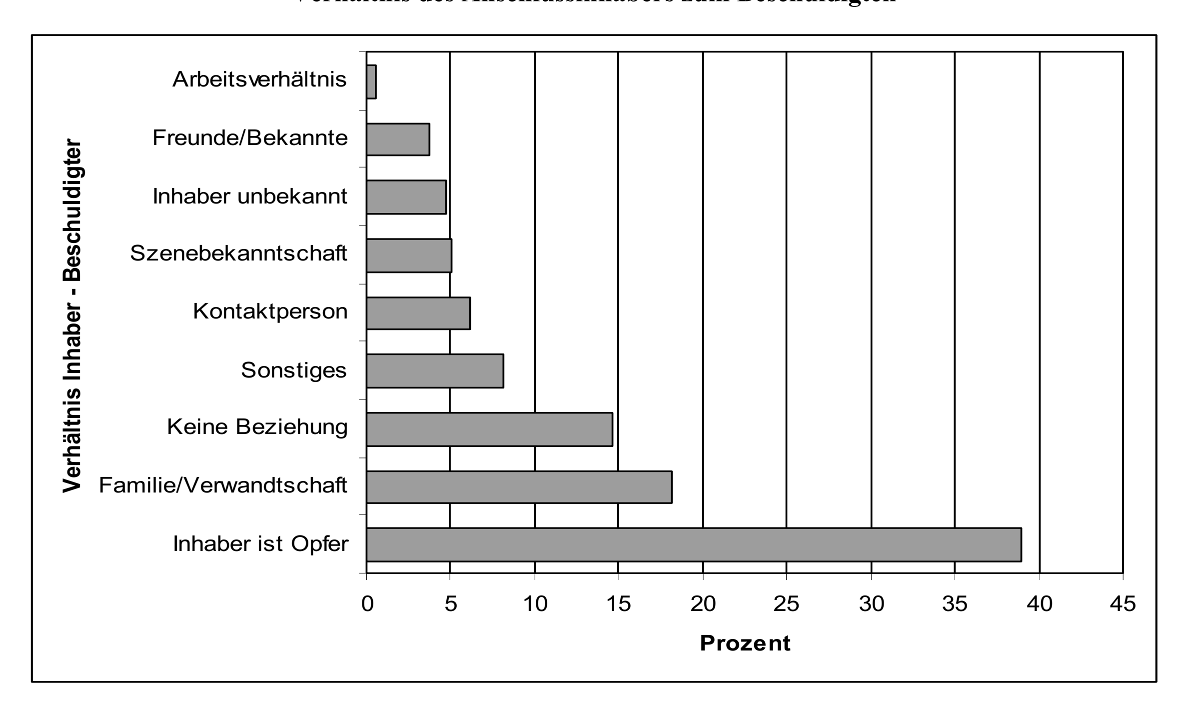


Abbildung 81

Verhältnis des Anschlussinhabers zum Beschuldigten



Bei 76 Anschlüssen gab es noch weitere Anschlussinhaber bzw. -nutzer, die von den Maßnahmen mit betroffen waren. Dabei handelte es sich in 54 Fällen um Ehepaare, in fünf Fällen ging es um ein „Familientelefon“ und in den übrigen Fällen handelte es sich u. a. um Betriebsanschlüsse oder Firmentelefone.

Gerade im Hinblick auf die hohe Zahl von Fällen, in denen der Anschlussinhaber das Opfer war (326), wurde aufgenommen, ob der Überwachte mit der Maßnahme einverstanden ist. Explizit war dies in 96 Fällen den Akten zu entnehmen. In 83 Fällen (86 Prozent) lag ausdrücklich ein Einverständnis der Betroffenen mit der Maßnahme vor. In 13 Fällen (14 Prozent) wurde dieses explizit verneint.

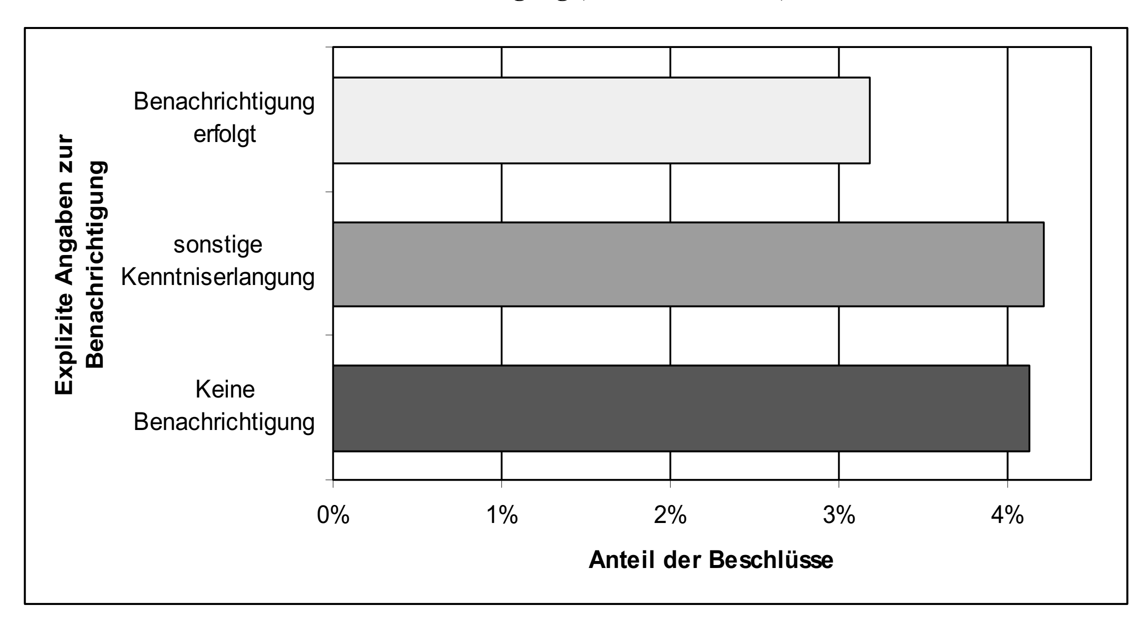
b) Benachrichtigung der Betroffenen

Bei 1105 von 1257 Beschlüssen waren den Akten keine Hinweise zur Benachrichtigung der Betroffenen über die Maßnahmen nach §§ 100g, 100h StPO zu entnehmen. Im Übrigen ließ sich den Akten – wie in Abbildung 82 dargestellt – entnehmen, dass bei 52 Beschlüssen (4 Prozent) ausdrücklich keine Benachrichtigung erfolgte. Bei 40 Beschlüssen wurde der Betroffene über die Verkehrsdatenabfrage (ggf. zusammen mit der Benachrichtigung über eine Telefonüberwachung) ausdrücklich benachrichtigt. Bei 53 Beschlüssen (4 Prozent) erlangte der Betroffene auf sonstige Weise Kenntnis (z. B. durch Vorhalt während der Vernehmung). Insgesamt erhielten 94 Personen auf diese Weise von den Maßnahmen Kenntnis. Zusätzlich ist zu berücksichtigen, dass bei etwa einem Drittel der von den Maßnahmen betroffenen Beschuldigten die Kenntnisnahme zumindest möglich war, da sie einen Verteidiger beauftragt hatten und dieser aufgrund seines Akteneinsichtsrechts Kenntnis von den Maßnahmen erlangen und seinen Mandanten darüber informieren konnte.

Gründe für die Nichtbenachrichtigung ließen sich den Akten bei 33 Beschlüssen entnehmen. Dabei war meistens die Gefährdung des Untersuchungszwecks ausschlaggebend. Bei fünf Beschlüssen wurde diesbezüglich der nicht einschlägige § 89 TKG (a. F.) von der Staatsanwaltschaft angeführt. In einem Fall unterblieb die Benachrichtigung zum Schutz einer V-Person.

Abbildung 82

Benachrichtigung (sofern ersichtlich)



3. Experteninterviews

a) Staatsanwälte

Die interviewten Staatsanwälte wurden gefragt, in welchem Umfang die Betroffenen von den Maßnahmen nach §§ 100g, 100h StPO benachrichtigt wurden. Etwas weniger als die Hälfte von ihnen bejaht dies im Grundsatz. Die Staatsanwaltschaft erlasse die Verfügung, dass ein Schreiben an den Anschlussinhaber geschickt werde. Das werde auch aktenkundig gemacht. Zwei dieser Befragten meinen aber, dass die Frage sei, wer unter den Begriff „Betroffener“ falle. Im Gesetz stehe „Beteiligter“. Dieser sei schwierig zu bestimmen. Benachrichtigt würden der Beschuldigte, der Anschlussinhaber und der Anschlussnutzer. Bei der Funkzellenabfrage würden aber nicht alle völlig Unbeteiligten benachrichtigt, die in der Funkzelle telefoniert hätten. Im Übrigen erfülle auch die Akteneinsicht die Benachrichtigungspflicht, sodass in diesen Fällen ebenfalls keine zusätzliche Benachrichtigung erfolge.

Ein Befragter schildert, dass allein die Mitteilung einer Rufnummer den Betroffenen nicht identifiziere. Denn der Betroffene sei nicht immer der Nutzer. Bei einem Handy werde der unbekannte Teilnehmer nicht benachrichtigt. Betroffene seien der Beschuldigte, Nachrichtenmittler sowie andere identifizierte Gesprächsteilnehmer. Zwei Befragte geben an, dass meist unklar sei, wer Anschlussinhaber sei. Es würden aber keine weiteren Ermittlungen in die Richtung durchgeführt, wer wirklich telefoniert habe. Personen alleine zum Zwecke der Benachrichtigung zu identifizieren sei nicht Praxis. Vier Befragte meinen, das komme darauf an. Meistens würden die Betroffenen benachrichtigt. Es werde bereits in den Ermittlungen an sie herangetreten (Vorhalt). Durch die Akteneinsicht der Verteidiger würden sie ebenfalls Kenntnis erlangen. Dann müssten sie nicht noch einmal gesondert benachrichtigt werden. Auch Geschädigte, die eine Zielwahlsuche wollten, seien ja bereits über die Maßnahme informiert. Zwei Befragte aus der Abteilung Computerkriminalität geben an, dass sie entweder mit unbekannten Personen zu tun hätten, welche nicht benachrichtigt werden könnten, oder mit bekannten Personen, die durch Akteneinsicht oder weitere Ermittlungen Kenntnis erlangen. Drei Befragte geben an, dass eine Benachrichtigung regelmäßig unterbleibe.

b) Verteidiger

Auch nach Ansicht der befragten Verteidiger wird die Benachrichtigung häufig durch die (beantragte) Akteneinsicht ersetzt. Die Betroffenen würden zumeist erst dann von der Maßnahme erfahren.

c) Datenschützer

Von zwei der befragten Datenschutzbeauftragten wurde geäußert, dass der Eindruck in den (wenn auch wenigen) von ihnen eingesehenen Akten entstehe, dass die Beteiligten nicht umfassend über die Maßnahme informiert würden. Zudem sei es vorgekommen, dass der Benachrichtigte „überschießende Informationen“, also z. B. auch die Anschlüsse anderer Verdächtiger mitgeteilt bekommen habe. Im Übrigen sahen sich die befragten Datenschutzbeauftragten zur Beurteilung der Frage, ob die Betroffenen benachrichtigt werden, außerstande, da ihnen zu wenig Datenmaterial zur Verfügung stehen würde. Wenn aber die Benachrichtigung schon nicht bei der Telekommunikationsüberwachung erfolge, dann erst recht nicht bei §§ 100g, 100h StPO. Es habe auch Fälle gegeben, in denen über die Durchführung der Telekommunikationsüberwachung benachrichtigt wurde, jedoch über die Verkehrsdatenabfrage nicht. Sie würden nur eingeschaltet von Betroffenen, die wüssten, dass eine Verkehrsdatenabfrage bei ihnen durchgeführt worden wäre. Auch einer der Datenschützer hält es für problematisch, wenn Personalien und Adresse nicht bekannt seien und extra ermittelt werden müssten, (nur) um der Benachrichtigungspflicht gerecht zu werden. Dann sei die Frage, ob der Eingriff durch die fehlende Benachrichtigung oder durch die Ermittlung der Personalien intensiver sei.

4. Zusammenfassung der Ergebnisse

Unmittelbar betroffen von der Verkehrsdatenabfrage sind die Inhaber der Anschlüsse sowie die Nutzer der Anschlüsse, zu denen Daten abgefragt werden. Nach den Ergebnissen der schriftlichen Befragung wurden im Durchschnitt 3,5 Betroffene pro Verkehrsdatenabfrage genannt. Bei der Auswertung der Akten konnten 1 645 Anschlussinhaber festgestellt werden, deren Anschlüsse unmittelbar betroffen waren. Davon waren 505 Beschuldigte und 1 110 Dritte. Etwa 70 Prozent der unmittelbar betroffenen und identifizierten Anschlussinhaber waren demnach Nichtbeschuldigte. Nutzer der Anschlüsse konnten bei 1 709 Anschlüssen festgestellt werden. In den übrigen Fällen war der Nutzer nicht ersichtlich. Bei 22 Prozent der Fälle, bei denen der Anschlussinhaber ein Dritter war, wurde der Anschluss ausschließlich vom Beschuldigten genutzt. Wenn es sich bei dem Inhaber des Anschlusses um einen Dritten handelte, war dies meistens das Opfer der Straftat (40 Prozent). Oft (18 Prozent) handelte es sich bei den Anschlussinhabern auch um Familienangehörige des Beschuldigten (Verwandte, Ehegatten, Schwager etc.). Weitere Inhaber bzw. Nutzer waren in 76 Fällen betroffen. Bei diesen handelte es sich überwiegend um den Ehegatten.

Der Anteil nicht benachrichtigter Betroffener wurde von den schriftlich Befragten im Mittel auf 38 Prozent geschätzt. Grund für die Nichtbenachrichtigung, der von den schriftlich befragten Staatsanwälten angeführt wurde, war vor allem die Gefährdung des Untersuchungszwecks. Es wurden aber auch der hohe Aufwand einer solchen Benachrichtigung sowie Arbeitsüberlastung von den Staatsanwälten angegeben. Zudem sei die Identität der Anschlussinhaber oftmals gar nicht bekannt und die Ermittlung des Anschlussinhabers, um die Benachrichtigungspflicht zu erfüllen, sei unverhältnismäßig. Weitere angegebene Gründe waren Vergesslichkeit, Nachlässigkeit und Versehen. Zudem erlange der Beschuldigte durch Vorhalt oder durch die Akteneinsicht seines Verteidigers Kenntnis von der Maßnahme. Die Mehrheit der schrift-

lich Befragten befürwortete die Einschränkung (33 Prozent) oder Abschaffung (45 Prozent) der Benachrichtigungspflicht. Die Auswertung der Akten ergab, dass in 87 Prozent der Beschlüsse den Akten keine Hinweise zur Benachrichtigung der Betroffenen zu entnehmen waren. In 3 Prozent der Beschlüsse erfolgte ausdrücklich eine Benachrichtigung, während in 4 Prozent ausdrücklich keine Benachrichtigung stattfand. Bei weiteren 4 Prozent erhielten die Betroffenen auf sonstige Weise Kenntnis von der Durchführung der Verkehrsdatenabfrage, etwa durch Vorhalt während der Vernehmung. Daneben ist zu berücksichtigen, dass bei etwa einem Drittel der von den Maßnahmen betroffenen Beschuldigten die Kenntnisnahme zumindest möglich war, da ihr Verteidiger im Wege der Akteneinsicht Kenntnis erlangen konnte. Gründe für die Nichtbenachrichtigung konnten den Akten bei 33 Beschlüssen entnommen werden, wobei hauptsächlich die Gefährdung des Untersuchungszwecks ausschlaggebend war. Ansonsten wurden noch auf datenschutzrechtliche Vorschriften des TKG verwiesen und die Benachrichtigung zum Schutz einer V-Person unterlassen. Die interviewten Staatsanwälte gaben etwa zur Hälfte an, dass eine Benachrichtigung regelmäßig erfolge. Problematisch sei aber, wer Betroffener sei. Völlig Unbeteiligte, deren Nummern bei einer Funkzellenabfrage auftauchen, würden nicht benachrichtigt werden. Zudem erfülle vielfach die Akteneinsicht des Verteidigers die Benachrichtigungspflicht. Die befragten Verteidiger sind der Ansicht, dass die Akteneinsicht die einzige Form der Benachrichtigung sei, die tatsächlich durchgeführt werde. Auch die befragten Datenschützer zweifeln an der Einhaltung der Benachrichtigungspflicht. Allerdings wird zu Bedenken gegeben, dass bei einem unbekannten Anschlussinhaber der Eingriff durch die Ermittlung seiner Identität zwecks Benachrichtigung größer sein könnte als das Unterlassen der Benachrichtigung.

VIII. Zeugnisverweigerungsrechte

1. Schriftliche Befragung

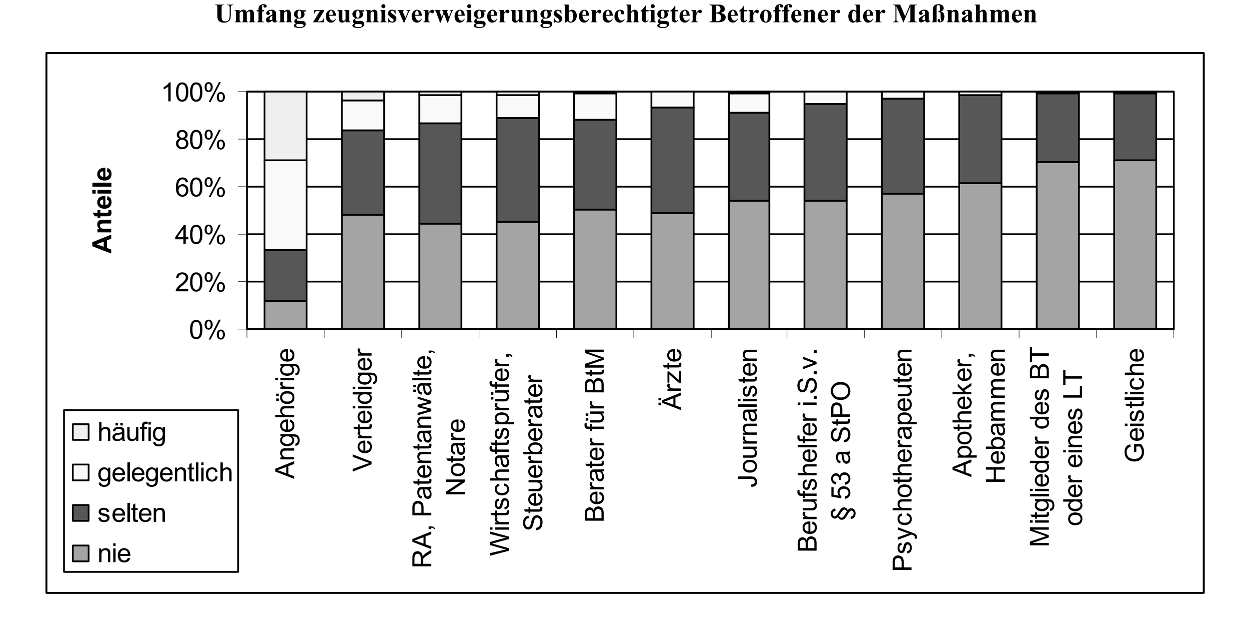
a) Zeugnisverweigerungsberechtigte Betroffene

In welchem Umfang zeugnisverweigerungsberechtigte Personen von Verkehrsdatenabfragen betroffen waren, beantworteten die schriftlich Befragten wie in Abbildung 83 veranschaulicht.

Häufig (29 Prozent) und gelegentlich (37 Prozent) betroffene Zeugnisverweigerungsberechtigte waren nach Angabe der Befragten einzig die Angehörigen i. S. v. § 52 StPO. Es folgen Verteidiger, sonstige Rechtsanwälte, Patentanwälte, Wirtschaftsprüfer und Steuerberater, die im Durchschnitt selten (41 Prozent) oder gelegentlich bis häufig (13 Prozent) betroffen waren. Von Ärzten und Beratern (Betäubungsmittel) wurde schon zu ca. 50 Prozent angegeben, dass sie nie betroffen seien (ca. 40 Prozent selten und 10 Prozent gelegentlich). Die weiteren Berufsgruppen sind in zunehmendem Maße nicht betroffen, Journalisten und Berufshelfer (nie ca. 54 Prozent), Psychotherapeuten (nie 57 Prozent), Apotheker, Hebammen (nie 62 Prozent), Mitglieder des Bundes- o. Landtags (nie 70 Prozent) und schließlich Geistliche (nie 71 Prozent). Demnach sind nach Einschätzung der Staatsanwälte zwei der Berufsgruppen, die von dem Verwertungsverbot des § 100h II StPO erfasst sind (Mitglieder des Bundestages und des Landtages sowie Geistliche), seltener tatsächlich Betroffene als andere Berufsgruppen, die nicht in § 100h II StPO aufgeführt sind.

Abbildung 83

Umfang zeugnisverweigerungsberechtigter Betroffener der Maßnahmen



b) Erweiterung des § 100h II StPO

Es wurde die Frage gestellt, ob die Zeugnisverweigerungsrechte aller Personen i. S. v. §§ 52, 53, 53a StPO in § 100h II Satz 1 StPO einheitlich berücksichtigt werden sollten. Dies befürworteten 37 Prozent der Befragten, wobei die Hälfte ihre Antwort begründete. Als Begründung wurde angegeben, dass es keinen Grund für eine Differenzierung bzw. Ungleichbehandlung gebe (31 Prozent). Weiter wurde angeführt, dass Einheitlichkeit zu befürworten sei und dies der Rechtssicherheit und Rechtsklarheit diene (26 Prozent). Weitere 19 Prozent gaben an, dass dies aus Gründen der Vereinfachung der Gesetzesanwendung geboten sei. Eine einheitliche Regelung sei übersichtlicher. Weitere Begründungen waren, dass sonst diese Zeugnisverweigerungsrechte umgangen würden, Wertungswidersprüche entstünden und der Schutzbereich und die Konfliktsituation bei den Gruppen gleich seien.

Von denjenigen, die eine einheitliche Berücksichtigung ablehnen (63 Prozent der Befragten), gab ebenfalls etwa die Hälfte eine Begründung ab. Am häufigsten wurde genannt, dass die Zeugnisverweigerungsrechte unterschiedlicher Natur seien (30 Prozent). Der Schutzzweck, die Interessenkollisionen und die Gründe für die Zeugnisverweigerungsrechte seien verschieden. 19 Prozent gaben an, dass die Ermittlungen bzw. die Aufklärung von Straftaten bei einheitlicher Berücksichtigung erheblich erschwert oder gar unmöglich würden. In die gleiche Richtung geht das Argument von weiteren 9 Prozent, die der Meinung sind, dass der Anwendungsbereich zu sehr eingeschränkt werde und die Maßnahme dadurch nahezu leer liefe. Eine Vereinheitlichung sei zu weitgehend und §§ 100g, 100h StPO sonst nicht mehr praktikabel. Auf diese Weise sei eine Umgehung der Verkehrsdatenabfrage möglich. 10 Prozent sind der Ansicht, dass die bestehende Regelung ausreichend sei und 8 Prozent finden die Differenzierung zwischen den Zeugnisverweigerungsrechten und die unterschiedliche Berücksichtigung sinnvoll. Ein weiterer Aspekt, auf den die Befragten hinwiesen, ist, dass das Zeugnisverweigerungsrecht vor Durchführung der Maßnahme oftmals gar nicht erkennbar sei (6 Prozent). Zudem wurde angeführt, dass Täter häufig die Anschlüsse ihrer Angehörigen benutzen (6 Prozent). Demnach wäre bei einer Berücksichtigung der Angehörigen in § 100h StPO der Anwendungsbereich der Verkehrsdatenabfrage stark eingeschränkt. Weitere Begründungen waren, dass sich die derzeitige Regelung bewährt habe, dass eine einheitliche Berücksichtigung der Zeugnisverweigerungsberechtigten nicht erforderlich sei und kein Bedarf dafür bestehe. Die Aufklärung von Straftaten gehe vor. Zumindest Angehörige sollten nicht in § 100h StPO berücksichtigt werden.

2. Aktenanalyse

a) Anteil betroffener Berufsgeheimnisträger und Berufshelfer

Den Akten war kein einziger Fall zu entnehmen, in dem ein Berufsgeheimnisträger oder Berufshelfer von der Verkehrsdatenabfrage betroffen war. Insbesondere gab es keinen Fall, in dem ein Geistlicher, Bundestags- oder Landtagsabgeordneter oder Strafverteidiger von der Maßnahme betroffen war. Dementsprechend lag auch in keinem Fall ein Verwertungsverbot i.S.v. § 100h II StPO vor. Es ist jedoch zu berücksichtigen, dass mit den Maßnahmen eine Vielzahl von Rufnummern oder IMEI-Nummern überprüft werden, ohne dass bekannt wird, wer die Anschlussinhaber hinter diesen Nummern sind. Nur bei Nummern, die in der Masse der Daten auffallen, wird weiter ermittelt, welcher Person diese zuzuordnen sind. Auffallen kann eine Rufnummer z. B. dann, wenn schon aus anderen Gründen ein Verdacht gegen den Inhaber der Nummer vorliegt oder wenn die Nummer bereits bei einem anderen ähnlichen Vorfall, der zum Vergleich herangezogen wird, auftaucht (z. B. bei mehreren Banküberfällen). Zudem kann z. B. bei einer Beleidigung per Telefon der Tatzeitraum vom Opfer eingegrenzt werden, so dass die anderen Rufnummern, die auf dem Einzelverbindungsnachweis zu einem anderen Datum und einer anderen Uhrzeit erscheinen, nicht näher untersucht werden. Dann sind die Inhaber dieser anderen Rufnummern aber auch nicht in dem Sinne der Vorschriften „betroffen“. Ihre Nummer gelangt zwar zur Kenntnis, was einen gewissen Grundrechtseingriff darstellt. Ihre Identität ist jedoch meist unbekannt. In den ausgewerteten Akten gab es keinen einzigen Fall, wo ausdrücklich die Daten des Anschlusses eines Zeugnisverweigerungsberechtigten i. S. v. §§ 53, 53a StPO abgefragt wurden.

b) Anteil betroffener zeugnisverweigerungsberechtigter Angehöriger

Die einzigen zeugnisverweigerungsberechtigten Personen, deren Anschlüsse ausdrücklich abgefragt wurden, sind Angehörige i. S. v. § 52 StPO. Es wurden Anschlüsse von Verwandten, dem Ehegatten und Verlobten überwacht. Zu den 1 909 Anschlüssen, für die Daten abgefragt wurden, ist den Akten in 1 645 Fällen ein Anschlussinhaber zu entnehmen gewesen (siehe dazu Abschnitt Betroffene). Davon sind 133 zeugnisverweigerungsberechtigt (8 Prozent). Bei diesen handelte es sich bei jeweils 45 um Verwandte und um den Ehegatten und bei fünf um den oder die Verlobte. In 94 Prozent dieser Fälle war dieses Zeugnisverweigerungsrecht auch vor Durchführung der Maßnahme ersichtlich. Ein Verwertungsverbot i. S. v. § 100h II StPO lag in keinem Fall vor.

3. Experteninterviews

a) Polizeibeamte

Die befragten Experten wurden nach Fällen gefragt, in denen zeugnisverweigerungsberechtigte Personen, insbesondere Journalisten, von der Verkehrsdatenabfrage betroffen waren. Ein solcher Fall ist keinem der befragten Polizisten bekannt. Ein Befragter gibt an, dass der Status einer Person meist nicht bekannt sei. Es wird weiter davon ausgegangen, dass Staatsanwaltschaft und Gericht dies berücksichtigen. Dass ein Verteidiger betroffen war, sei lediglich im Zusammenhang mit einer Telekommunikationsüberwachung vorgekommen. Die Gespräche seien dann nicht verwertbar gewesen.

Keiner der Befragten würde eine Erweiterung des Verwertungsverbots des § 100h II StPO auch auf andere Zeugnisverweigerungsberechtigte befürworten. Begründet wurde dies u. a. damit, dass die Lage der §§ 52, 53 StPO hier nicht gegeben sei. Eine Ausdehnung würde die polizeiliche Arbeit nur erschweren und sei nicht gerechtfertigt. Gerade bei Journalisten sei ein solches Privileg nicht wünschenswert. Täter würden sich erfahrungsgemäß häufig an diese wenden, um die Tat öffentlich zu machen. Ein weiterer Befragter gab an, dass die Regelung seiner Meinung nach schon heute zu weit gefasst sei. Richter und Staatsanwälte seien zudem sensibel genug. Man könne erst nach der Auswertung der Daten feststellen, wer tatbeteiligt ist. Im Rahmen der Verhältnismäßigkeit könnte man dann weitere Personen einbringen, aber ein absolutes Verwertungsverbot für alle sei nicht wünschenswert.

b) Staatsanwälte

Fälle, bei denen die Verkehrsdaten von Journalisten abgefragt wurden, sind auch keinem der befragten Staatsanwälte bekannt. Eine Erweiterung des Verwertungsverbots auch auf andere Zeugnisverweigerungsberechtigte befürworten die meisten befragten Staatsanwälte ebenfalls nicht. Die bestehende Regelung sei ausreichend und ein Bedürfnis für eine Erweiterung nicht erkennbar, zumal es schon genügend Einschränkungen gebe. Dadurch gingen nur Erkenntnismöglichkeiten verloren. Insgesamt wird freilich die Inkongruenz der Regelungen der Verwertungsverbote bei den verschiedenen verdeckten Ermittlungsmaßnahmen kritisiert. Eine Vereinheitlichung sei wünschenswert. Ein Befragter hätte gegen eine Erweiterung auf Rechtsanwälte keine Bedenken. Bezüglich Journalisten äußert er sich aber eher skeptisch. Das sei zu weitgehend.

c) Richter

Auch die befragten Ermittlungsrichter haben nach eigenen Angaben keine Fälle bearbeitet, in dem die Verkehrsdaten von Journalisten abgefragt wurden. Ein Befragter gibt an, dass dies meist nicht ersichtlich sei, da oft kein Name, sondern nur eine Telefonnummer bekannt sei. Aber ggf. seien die Daten dann im Nachhinein nicht verwertbar. Ein sensibler Umgang mit diesen Daten sei notwendig, aber nicht immer einfach.

Über die Hälfte der Befragten sprach sich gegen eine Erweiterung des § 100h II StPO auch auf andere Zeugnisverweigerungsberechtigte aus. Die derzeitige Regelung sei ausreichend. Ein Befragter erläutert, dass er das Zeugnisverweigerungsrecht bei Pastoren verstehen könne, aber bei Journalisten nicht. Ein anderer meint, es sei die Frage, wo die Grenze zu ziehen sei. Straftäter würden eben über Mobiltelefone von Verwandten telefonieren. In einem solchen Fall sei eine Begrenzung z. B. auf ein paar Tage sinnvoll, um herauszubekommen, ob der Täter das Mobiltelefon überhaupt nutze. Zwei der befragten Richter geben an, dass ihnen nicht klar sei, warum gerade diese Zeugnisverweigerungsberechtigten von § 100h II StPO erfasst würden. Bei jedem Zeugnisverweigerungsrecht stehe das Recht des Zeugnisverweigerungsberechtigten gegen die Sachaufklärung. Eine Ausdehnung führe daher nur zur Behinderung der Aufklärung. Es gebe Fälle, in denen ein Tatvorwurf wegen der Zeugnisverweigerungsrechte fallengelassen werden müsse. Andererseits sei dieses Recht bei Ärzten und Rechtsanwälten gerechtfertigt. Bei Wirtschaftsprüfern und Steuerberatern dagegen sei im Einzelfall abzuwägen. Schließlich würden zwei der befragten Ermittlungsrichter eine Erweiterung befürworten. Das Zeugnisverweigerungsrecht solle nicht ausgehebelt werden.

d) Verteidiger

Auf die Frage, ob es im Rahmen ihrer Tätigkeit vorgekommen sei, dass die Verkehrsdaten von Journalisten oder sonstigen Zeugnisverweigerungsberechtigten abgefragt wurden, konnten von Verteidigerseite nur Abfragen der Daten von Angehörigen angegeben werden. Andere Fälle seien nicht vorgekommen. Alle Befragten würden eine Erweiterung des Verwertungsverbots des § 100h II StPO auf andere Zeugnisverweigerungsberechtigte befürworten. Ein Verteidiger ist der Ansicht, dass alle auch sonst Zeugnisverweigerungsberechtigten erfasst werden sollten, um Umgehungen auszuschließen. Ein anderer Befragter hält die Einbeziehung von Berufsgeheimnisträgern für sinnvoll. Weiter wird dafür plädiert, dass Journalisten und Angehörige erfasst sein sollten. Wichtig sei vor allem auch die Berücksichtigung von Drogenberatern. Deren Tätigkeit könnte durch die Gefahr der Überwachung beeinflusst werden.

e) Datenschützer

Auch die Datenschutzbeauftragten befürworten durchweg eine Erweiterung des Verwertungsverbots des § 100h II StPO auch auf andere Zeugnisverweigerungsberechtigte. Unterschiedliche Meinungen wurden allerdings offenbar, wer konkret berücksichtigt werden sollte. Ein Befragter gab an, dass alle Zeugnisverweigerungsberechtigten des § 53 StPO berücksichtigt werden sollten. Sonst würde das Recht des § 53 StPO ausgehöhlt werden. Ein anderer ist der Ansicht, dass ein möglichst großer Teil berücksichtigt werden sollte, dies aber angesichts der Rechtsprechung des Bundesverfassungsgerichts nicht durchsetzbar sei. Das Bundesverfassungsgericht gebe eine Differenzierung vor, nach der Journalisten nur bedingt zeugnisverweigerungsberechtigt seien. Zwei der Befragten wollen den Schutz des § 100h II StPO auf jeden Fall auf Ärzte, Psychotherapeuten, Drogenberater und andere Beratungsstellen ausdehnen. Hier bestehe ein erheblich gesteigertes Bedürfnis nach Vertraulichkeit. Immer wenn ein gesteigerter Sensibilitätsgrad gegeben sei, sollten erhöhte Anforderungen an ein Auskunftsverlangen gestellt werden. Zudem sei nicht einleuchtend, warum die Schutzwürdigkeit bei anderen Rechtsanwälten als Strafverteidigern geringer sein solle. Eine klare Abgrenzung könne ohnehin problematisch sein. Bei Journalisten gestalte sich die Lage nach Ansicht eines Befragten freilich etwas anders. Hier gehe es nicht um Menschenwürde, sondern um Pressefreiheit und Informantenschutz.

4. Zusammenfassung der Ergebnisse

Die am häufigsten von der Verkehrsdatenabfrage betroffenen Zeugnisverweigerungsberechtigten sind nach Angabe der schriftlich befragten Staatsanwälte die Angehörigen i. S. v. § 52 StPO. Verteidiger, sonstige Rechtsanwälte, Wirtschaftsprüfer etc. seien eher seltener betroffen. Mitglieder des Bundestages oder eines Landtages sowie Geistliche sollen nach den meisten Befragten nie betroffen sein. Dieses Ergebnis wird durch die Ergebnisse der Aktenanalyse bestätigt. Den Akten war kein Fall zu entnehmen, bei dem ein Berufsgeheimnisträger oder Berufshelfer betroffen war. Demnach bestand auch in keinem Fall ein Verwertungsverbot i. S. v. § 100h II StPO. Zu berücksichtigen ist allerdings, dass eine Vielzahl von Rufnummern durch die Verkehrsdatenabfragen mit betroffen ist, hinter denen sich unerkannt durchaus Berufsgeheimnisträger verbergen können. 133 Anschlussinhaber waren tatsächlich zeugnisverweigerungsberechtigt gemäß § 52 StPO. Der Großteil davon waren Verwandte oder Ehegatten. Den interviewten Experten war kaum ein Fall bekannt, in dem eine Berufgeheimnisträger betroffen war von den Maßnahmen nach §§ 100g, 100h StPO.

37 Prozent der Teilnehmer an der schriftlichen Befragung würden eine einheitliche Berücksichtigung von Zeugnisverweigerungsberechtigten befürworten, 63 Prozent dagegen lehnen eine solche Vereinheitlichung ab. Auch die Ergebnisse der mündlichen Befragungen bestätigen dieses Bild. Alle befragten Polizeibeamten und die meisten befragten Staatsanwälte lehnen eine Erweiterung des Verwertungsverbots des § 100h II StPO ab. Dies würde die Ermittlungstätigkeit nur erschweren. Eine Vereinheitlichung der Verwertungsverbote bei verdeckten Ermittlungsmaßnahmen sei jedoch wünschenswert. Auch über die Hälfte der befragten Richter ist gegen eine Berücksichtigung weiterer Zeugnisverweigerungsberechtiger. Andere meinen, dass Ärzte und Rechtsanwälte berücksichtigt werden könnten. Dagegen waren alle befragten Verteidiger sowie die interviewten Datenschützer für eine einheitliche Regelung. Mehrfach wird angeführt, dass gerade Ärzte, Psychotherapeuten, Drogenberater oder ähnliche Beratungsstellen berücksichtigt werden sollten.

IX. Kosten

Ein wichtiges Thema – gerade für die Telekommunikationsunternehmen – sind die bei der Durchführung der Maßnahmen entstehenden Kosten.

1. Schriftliche Befragung

Die mittels Fragebogen befragten Staatsanwälte sollten schätzen, wie hoch die Kosten, die den Netzbetreibern durch die Maßnahmen nach §§ 100g, 100h StPO entstehen, sind. Etwa 40 Prozent der Befragten gaben einen konkreten Betrag an. Dabei fiel auf, dass sowohl Beträge bis zu 300 Euro (90 Prozent der Angaben), aber auch wesentlich höhere Kosten bis zu 50 000 000 Euro geschätzt wurden. Offensichtlich wurde die Frage zwar zum größten Teil als Kostenschätzung für *eine* Maßnahme verstanden, aber es wurden auch Gesamtkosten aller Maßnahmen geschätzt. Berücksichtigt man nur die Schätzungen bis zu 300 Euro, so ergibt sich ein Mittelwert von 66 Euro (Median 50 Euro). Am häufigsten wurden Beträge von 20 bis 30 Euro, 50 Euro und 100 Euro angegeben. Eingestuft wurden die Kosten als eher niedrig (54 Prozent, niedrig 17 Prozent, eher hoch 18 Prozent)[450].

Ob der Kostenaspekt eine Rolle für die Befragten selbst bei der Beantragung der Verkehrsdatenabfrage spielt, bejahten diese zu 14 Prozent. Häufigste Begründung dafür war, dass der Verhältnismäßigkeitsgrundsatz auch im Hinblick darauf zu beachten sei (24 Prozent). 16 Prozent dieser Personen führten aus, dass unnötige Kosten vermieden werden müssten. 13 Prozent gaben an, dass Kosten immer zu berücksichtigen seien. Es herrsche eine angespannte Finanzlage und die Kosten, die durch die Maßnahmen entstünden, seien hoch (10 Prozent der Befragten dieser Gruppe). Weitere wurde ausgeführt, dass das Kosten-Nutzen-Verhältnis stets zu beachten sei (7 Prozent). Einige der Befragten führten außerdem aus, dass sie Kosten nur berücksichtigen, wenn geringfügige Delikte Gegenstand des Verfahrens sind (6 Prozent). Diejenigen, für die der Kostenaspekt keine Rolle spielt (86 Prozent), begründeten dies größtenteils damit, dass die Aufklärung der Straftat bzw. der Ermittlungserfolg im Vordergrund stehe (20 Prozent dieser Befragten, Mehrfachnennungen möglich). Die Strafverfolgung sollte nicht von Kosten abhängig sein (17 Prozent). Weitere 5 Prozent stellten diesbezüglich besonders auf die Aufklärung erheblicher Taten ab. 12 Prozent beriefen sich als Begründung auf das Legalitätsprinzip und 2 Prozent auf den Amtsermittlungsgrundsatz. 7 Prozent argumentieren, es gehe um Straftaten von erheblicher Bedeutung und nicht um Bagatellen. Weiter wurde angeführt, dass die Kosten für die Verkehrsdatenabfrage in der Regel ohnehin gering seien (10 Prozent). 8 Prozent gaben an, dass ein Antrag nach §§ 100g, 100h StPO nur erfolge, wenn die Maßnahme erforderlich sei und kein milderes Mittel vorhanden. Ebenso sind 6 Prozent der Ansicht, dass es oftmals keine anderen Ermittlungsansätze gebe und somit die Auskunft über die Daten die einzige Möglichkeit sei. Die Maßnahme sei notwendig (6 Prozent) und die Taten sonst nicht aufklärbar (5 Prozent). Schließlich wurde angeführt, dass die Strafprozessordnung die Berücksichtigung der Kosten bei der Beantragung nicht vorsehe. Ermittlungen würden stets Kosten auslösen und Strafverfolgung könnte nicht unter ökonomischen Gesichtspunkten durchgeführt werden. Mögliche Ermittlungsmaßnahmen müssten ausgeschöpft werden.

2. Aktenanalyse

Bei ca. einem Drittel der Beschlüsse konnten den Akten Angaben zu den Kosten entnommen werden. Sie reichten von 7 Euro bis 800 Euro. Im Mittel beliefen sich die Kosten auf 85 Euro (Median: 66 Euro) pro Beschluss. Soweit Zahlungen den Akten zu entnehmen waren (drei Viertel

[450] Diese Einschätzung ist im Wesentlichen unabhängig davon, ob die Gesamtkosten oder die Kosten für eine einzelne Maßnahme geschätzt wurden.

dieser Fälle), wurden diese Kosten den Anbietern ersetzt. Die Kosten pro Verfahren lagen, soweit bekannt (ca. bei der Hälfte der Verfahren), im Mittel bei ca. 140 Euro. Diese wurden – soweit dies nachvollzogen werden konnte – größtenteils ersetzt. Zu berücksichtigen ist hier, dass die Akten nicht immer die Rechnungen der Anbieter enthielten. In vielen Akten waren gar keine oder nur ein Teil der Rechnungen vorhanden[451]. Teilweise wurden die Kosten für Telekommunikationsüberwachungsmaßnahmen und Verkehrsdatenabfrage zusammen in Rechnung gestellt und konnten nicht auseinandergerechnet werden. Hinsichtlich der Bezahlung der Rechnungen, welche durch die Staatsanwaltschaft oder durch die Polizei erfolgte, konnten den Akten nur Indizien entnommen werden. So wurde festgehalten, ob eine Prüfung der Kostenhöhe vermerkt wurde und eine Kostenanweisung erfolgte. Aus diesen Hinweisen kann allerdings kein Nachweis darüber erbracht werden, ob die Kosten tatsächlich bezahlt wurden. Wie bei den Interviews mit den Telekommunikationsanbietern deutlich werden wird, kommt es den Anbietern auch nicht auf den Ersatz des in Rechnung gestellten Betrages an. Fast alle Anbieter führten aus, dass diese in Rechnung gestellten Kosten vollständig ersetzt werden. Den Anbietern geht es vielmehr um die Kosten, die sie nach den gesetzlichen Vorschriften nicht in Rechnung stellen dürfen.

3. Experteninterviews

a) Telekommunikationsunternehmen

(1) Kosten

(a) Kosten pro Maßnahme

Die befragten Unternehmen gaben übereinstimmend an, dass die Kosten für eine einzelne Auskunftserteilung nicht genau benannt werden könnten. Für die Kostenermittlung komme es darauf an, um welchen Typ von Abfrage es sich handle. Eine Auskunftserteilung könne für eine oder 50 Nummern erfolgen. Berechnet wird von allen Anbieter der Höchstbetrag gem. JVEG (§ 23 I Nr. 3 JVEG) in Höhe von 17 Euro pro Arbeitsstunde zuzüglich Versandpauschale. Diese 17 Euro würden den Aufwand bzw. die bei den Unternehmen tatsächlich entstandenen Kosten jedoch keinesfalls decken. Allein die Personalkosten für eine Arbeitsstunde würden diesen Betrag deutlich überschreiten. Die Anbieter gaben Beträge von 50 Euro, 71 Euro, 75 Euro und 85 Euro für eine Arbeitsstunde an. Nicht erfasst würden darüber hinaus Sachmittel, also Bürokosten für PC, Fax, Papier, etc. Kosten für organisatorische Vorkehrungen und Schulungen (juristische und technische Seminare) würden ebenfalls nicht erstattet. Auch die Investitionskosten für die Hardware dürften per Gesetz nicht in Rechnung gestellt werden, die ebenfalls einen hohen Betrag ausmachten. Ein Befragter meint, dass eine Pauschalierung im JVEG oder TKG bzgl. der Kosten ideal wäre. Eine Zeitabrechnung pro Maßnahme wird nicht für optimal gehalten, da in diesem Fall Disketten, Materialkosten etc. nicht mit berechnet werden könnten.

(b) Jährliche Kosten

Die Entwicklung der jährlich entstehenden Kosten konnte von den Anbietern nicht angegeben werden, da keine Statistik über die Kosten, die speziell für die Verkehrsdatenabfrage entstünden, geführt werde. Fast alle Befragten konnten aber Angaben zu den aktuell bzw. im Jahr 2005 entstandenen Kosten machen. Vodafone gibt an, dass dem Unternehmen im Jahr 2005 für Anordnungen nach §§ 100g, 100h StPO Kosten in Höhe von 2,5 Millionen Euro entstanden seien. Das sei eine 42 Prozentige Steigerung zum Vorjahr. Die Unterdeckung der Kosten für die Maßnahmen nach §§ 100g, 100h StPO und für Telekommunikationsüberwachungsmaßnahmen würde sich im Millionen-Bereich bewegen, und das ohne Berücksichtigung der Kosten für die Hardware. Immerhin würden die Rechnungen seit der Umstellung auf ZSEG bzw. JVEG zu fast 100 Prozent ersetzt. E-Plus schildert, dass ein System für §§ 100g, 100h StPO und § 113 TKG eingesetzt werde, das ständig fortentwickelt werde und der Wartung unterliege (20 Prozent Bestandsdaten; 80 Prozent Verkehrsdaten). Die Wartungskosten beliefen sich nach den Angaben auf 50 000 Euro, die Kosten für die Fortentwicklung auf 100 000 bis 150 000 Euro. Hinzu kämen ferner Investitionen zwischen 300 000 und 400 000 Euro. Ein Sachbearbeiter koste etwa 640 Euro pro Tag und Person (Büropauschalen). Ersetzt werde für §§ 100g, 100h StPO nur der reine Zeitaufwand. Etwa 80 Prozent der Rechnungen würden ersetzt. O2 gibt an, dass für alle Behördenauskünfte Kosten von mehr als 7 Millionen Euro pro Jahr entstehen würden. 4,2 Millionen Euro entfielen dabei auf §§ 100gh-Maßnahmen und Bestandsdaten (Datenbank, Personal, etc.). In Rechnung gestellt worden seien für §§ 100g, 100h StPO im Jahr 2005 aber nur 207 000 Euro. Davon seien 95 Prozent von den Behörden bezahlt worden. Bestandsdatenabfrage und Verkehrdatenabfrage stünden dabei in einem Verhältnis von 37 Prozent (Bestandsdatenabfrage) zu 63 Prozent (Verkehrsdatenabfrage). Die T-Com führt aus, dass §§ 100g, 100h-Anordnungen und Telekommunikationsüberwachungsmaßnahmen nicht separat erfasst würden. Insgesamt seien 4½ Millionen Euro im Jahr 2005 an reinen Personalkosten durch diese Maßnahmen entstanden, und zwar ohne technische Investitionen. Letztere hätten Ausgaben in Höhe von 25 Millionen Euro verursacht. Für die Upgrades der Software entstünden 1,5 Millionen Euro Kosten pro Jahr. Diese Kosten fielen nur für die Überwachungsmaßnahmen an, vor allem jedoch für die Umsetzung von Anordnungen nach § 100a StPO. Teilweise würden auch noch die Geschäfte von kleinen Anbietern mitbearbeitet bzw. diesen würde die Plattform des Unternehmens eingeräumt, da sich kleine Unternehmen die Bearbeitung alleine gar nicht leisten könnten. In der Regel würden die Rechnungen ersetzt. T-Mobile führt aus, dass neun Personen im operativen Bereich beschäftigt würden, bei 80 Euro pro Arbeitsstunde. Dadurch entstünden 1,2 Millionen Euro Personalkosten. Applikation und Weiterentwicklung führten zum Einsatz von etwa einer Mil-

[451] Kostenhefte konnten aus Zeitgründen nicht in allen Fällen eingesehen werden.

lion Euro pro Jahr. Ingesamt würden die Anordnungen nach §§ 100g, 100h StPO etwa 2 ½ Millionen Euro pro Jahr kosten. Davon seien im Jahr 2005 600 000 Euro ersetzt worden. Die in Rechnung gestellten Kosten würden von den Behörden überwiegend bezahlt. Arcor konnte keine Angaben zu den Kosten machen. Man schätzt aber, dass weniger als 50 Prozent der Rechnungen von den Behörden bezahlt würden. Die Befragten gaben größtenteils an, dass die Rechnung an denjenigen geschickt würde, der in der Anfrage als Rechnungsempfänger genannt würde. Wenn ein Rechnungsempfänger im Anschreiben nicht genannt werde, gehe die Rechnung an den Anfragenden. Die Bezahlung sei landesspezifisch geregelt. Rechnungsempfänger seien in den meisten Bundesländern die Staatsanwaltschaft, teilweise die Polizei, selten die Gerichte. Bei den Anbietern, die an der ESB angeschlossen seien, komme es für den Zentralen Polizeidienst Duisburg und das Landeskriminalamt Bayern zu Sammelrechnungen.

(2) Veränderungen des Unternehmens durch die Zunahme der Anfragen

(a) Erweiterung der Abteilungen

Alle Befragten gaben an, dass die Abteilungen aufgrund der Zunahme der Anordnungen erweitert worden wären. Bei einem Unternehmen erhöhte sich die Anzahl der in dieser speziellen Abteilung Beschäftigen von einem auf vier Mitarbeiter. Dies habe aber mit der erhöhten Zahl von Auskunftsersuchen generell zu tun. Der Mitarbeiter eines anderen Unternehmens gab an, dass die Abteilung mit stetig steigenden Zahlen der Anfragen immer mehr Mitarbeiter eingestellt habe. Ursprünglich hätten drei Personen in diesem Bereich gearbeitet. Die Mitarbeiteranzahl sei nunmehr auf 18 gestiegen. Bei einem anderen Telekommunikationsunternehmen bestehe, nach Angaben eines Mitarbeiters, im Schnitt eine jährliche Steigerung der Anordnungen um etwa 30 Prozent. Das führe zu regelmäßigem Personalaufbau. 1999 seien drei Personen damit beschäftigt gewesen, nunmehr seien es zwölf. Ein weiterer Befragter aus einem anderen Unternehmen gibt an, dass seit 2003 die Personalstellen um 20 bis 30 Prozent erhöht worden seien. Das hinge auch mit der Abfrage zu IP-Adressen zusammen. Der Mitarbeiter eines weiteren Unternehmens schildert, dass die Abteilung in der Zeit von 2001 bis 2004 einen Zuwachs von zwei auf zehn Mitarbeiter erfahren habe. Ein anderer Befragter führt aus, dass zunächst ein Mitarbeiter eingesetzt worden sei. Im Zuge des wachsenden Verkehrsaufkommens sei die Abteilung auf mittlerweile 17 Mitarbeiter angewachsen. In drei der befragten Unternehmen wurden Juristen für diese Abteilungen eingestellt. Ein Befragter gibt an, dass zunächst kein Jurist in der Abteilung gearbeitet hätte und ständiger Kontakt zur Rechtsabteilung hätte gehalten werden müssen. Daher habe man es sinnvoll gefunden, einen Juristen direkt in die Abteilung zu integrieren. Zudem erfolge nach Angabe von einem Befragten zusätzlich eine Abstimmung mit der Rechtsabteilung in besonderen Fällen.

(b) Zusammenhang mit den normalen Geschäftsabläufen

Ein Zusammenhang mit den normalen Geschäftsabläufen bestehe bei fast allen Befragten grundsätzlich nicht. Ganz im Gegenteil werden die Anordnungen für die Geschäftstätigkeit eher negativ bewertet. Die Kunden, so wird angenommen, würden weniger telefonieren, wenn Überwachungsmaßnahmen bekannt seien. Ein Befragter bejaht den Zusammenhang mit den normalen Geschäftsabläufen, da eine Speicherung nur zur Entgeltberechnung erfolge. Die Daten seien unverzüglich zu löschen, wenn sie dafür nicht mehr benötigt würden. Die gesetzliche Beauskunftung erfasse nur die Auskunft über das, was bereits gespeichert sei. Grundsätzlich sieht keines der Unternehmen ein Eigeninteresse an den Auskunftserteilungen. Teilweise würden die Einrichtungen bzw. Daten genutzt, meint einer der Befragten. Nur bei Betrugsfällen, die das Unternehmen betreffen, werde noch auf Verkehrsdaten zugegriffen, in dem Rahmen, in dem es gesetzlich möglich sei.

(c) Einfluss auf andere Unternehmensentscheidungen

Die Hälfte der Befragten gab an, dass die hohe Anzahl an Anordnungen auch für Unternehmensentscheidungen in anderen Bereichen eine Rolle spiele. Die Personal- und Budgetplanung sei davon betroffen. Gelder und Arbeitskräfte würden in anderen Bereichen und Arbeitskreisen abgezogen, wenn die Anfragen in der mit Telekommunikation befassten Abteilung stiegen. Neue Stellen könnten nur temporär besetzt werden. Die Anzahl der Anfragen bestimme z. B. die (hohe) Anzahl der Arbeitsplätze in der Abteilung. Bei der Planung bzgl. anderer Abteilungen müsse beachtet werden, dass die Überwachung in jedem Fall bestehen bleiben muss. Bei drei großen Unternehmen würden die Abfragen zwar bei der Personalplanung berücksichtigt, aber das Unternehmen werde ansonsten nicht davon beeinflusst. Aufgrund der Größe des Unternehmens hingen keine wirtschaftlichen Entscheidungen davon ab. Ob sich das Unternehmen insgesamt durch die Anordnungen verändert habe, verneinten alle Befragten grundsätzlich. Es habe nur Veränderungen in der Abteilung gegeben, wo mehr Personal eingesetzt worden sei, weil der Bereich der Überwachung größer werde. Darüber hinaus hätten die Anordnungen keine Bedeutung für das Unternehmen. Ein Befragter meint, dass sich das Problembewusstsein bzgl. der rechtlichen und technischen Fragestellungen erhöht habe. Veränderungen würden wohl eher bei kleineren Unternehmen auftreten. Grundsätzlich sehe man sich in einem Konflikt zwischen einem Verstoß gegen das Fernmeldegeheimnis und einem Verfahren wegen Strafvereitelung.

b) Polizeibeamte

Die interviewten Polizeibeamten wurden nach der Entschädigung der Netzbetreiber gefragt und ob es dabei Schwierigkeiten gegeben habe. Dies wurde unterschiedlich beantwortet. Vier der Befragten gaben an, dass sie dabei keine Probleme sehen würden. Es gebe keine gra-

vierenden Abrechnungsprobleme. Die Polizei bezahle die Rechnungen, nicht die Staatsanwaltschaft. Probleme ergäben sich in Bezug auf die Abrechnungshöhe. Teilweise würden überhöhte Rechnungen gestellt. Neuere Anbieter wollten nach Sachverständigenvergütung abrechnen, was aber eine fehlerhafte Auslegung des JVEG darstelle. Vereinzelt seien Rechnungen auch doppelt gestellt worden. Die Geschäftszeichen (Aktenzeichen der Polizei, Staatsanwaltschaft und des Gerichts) würden teilweise nicht übereinstimmen. Die Rechnungen seien zudem wenig transparent, man könne sie schlecht überprüfen. Früher seien „horrende Summen" in Rechnung gestellt worden. Ein Befragter gab an, dass er es als Bürgerpflicht ansehe, dass zur Strafverfolgung beigetragen werde. Die Provider sollten daraus keinen Profit schlagen können.

c) Staatsanwälte und Richter

Die befragten Staatsanwälte gaben überwiegend an, dass es hinsichtlich der Entschädigung der Anbieter keine Probleme gebe. Früher habe es ungerechtfertigte Forderungen gegeben. Das habe sich jedoch mittlerweile eingespielt. Teilweise wurde geschildert, dass die Rechnungen der Anbieter für die Abfragen an die Polizei gingen und diese oder die Staatsanwaltschaft sie bezahle. Die meisten Richter geben an, dass sie mit der Entschädigung der Netzbetreiber nichts zu tun hätten. Die Rechnungen würden grundsätzlich über die Staatsanwaltschaft bearbeitet. Das seien dann Kosten des Verfahrens. Beschwerden beträfen allenfalls Verzögerungen in der Begleichung der Rechnungen.

4. Zusammenfassung der Ergebnisse

Die Kosten, die im Rahmen der Durchführung einer Maßnahme nach §§ 100g, 100h StPO entstehen, wurden auf der Grundlage der von den Netzbetreibern zur Verfügung gestellten Informationen bestimmt. Aus den Akten ergeben sich teilweise die durch die Netzbetreiber in Rechnung gestellten Kostenbeträge. Soweit dies überhaupt aus den Akten ersichtlich war, beliefen sich die Kosten im Mittel auf 85 Euro pro Beschluss und auf etwa 140 Euro pro Verfahren. Diese Kosten wurden, soweit dies nachvollzogen werden konnte, größtenteils ersetzt. In den Akten waren jedoch nur teilweise die Rechnungen der Anbieter enthalten und der Ersatz der Rechnungen wurde anhand etwaiger Vermerke, dass die Kosten sachlich richtig berechnet seien und eine Kostenanweisung erfolge, festgehalten. Auch die Schätzung der schriftlich befragten Staatsanwälte hinsichtlich der Kosten der Verkehrsdatenabfrage spiegelt die Größenordnung des in Rechnung gestellten Betrages recht realistisch wieder. Im Mittel gaben die Befragten 66 Euro pro Maßnahme an. Der Kostenaspekt spielt nach der Angabe der meisten befragten Staatsanwälte (86 Prozent) keine Rolle bei der Beantragung der Maßnahmen. Die Aufklärung der Straftat stehe im Vordergrund und dürfe nicht von den Kosten abhängen. Diese im Rahmen der Aktenanalyse und der schriftlichen Befragung erhobenen Werte spiegeln jedoch nicht die Kosten wieder, die den Telekommunikationsanbietern nach deren Angaben für die Ausführung solcher Maßnahmen tatsächlich entstehen. Dies betrifft vor allem Personalkosten, Wartungskosten, Investitionskosten, Bürokosten, Kosten für organisatorische Vorkehrungen und Schulungen. Da die Entwicklung der Kosten für die Maßnahmen nach §§ 100g, 100h StPO nicht statistisch von den Anbietern festgehalten wird und zudem Verkehrsdatenabfragen, Behördenauskünfte und die Telekommunikationsüberwachung teilweise in einer Abteilung bearbeitet werden, ergeben sich unterschiedliche Kostenschätzungen. Die von allen Mitarbeitern der Unternehmen angegebene Unterdeckung der Kosten bewegt sich jedoch im Millionenbereich. Zudem seien die Abteilungen, in denen die Verkehrsdatenabfragen bearbeitet werden, wegen der steigenden Zahl von Anfragen erweitert worden. Teilweise arbeiten in diesen Bereichen bis zu 18 Personen, wobei aufgrund rechtlicher Probleme teilweise Juristen eingestellt wurden.

X. Vernichtung

Die Frage, ob die Verkehrsdaten vernichtet wurden, wenn ihre Speicherung nicht mehr erforderlich war, wurde in der Aktenanalyse und in den Gesprächen mit den Staatsanwälten thematisiert.

1. Aktenanalyse

In 3 Prozent der Verfahren konnte den Akten entnommen werden, dass die Daten nach Abschluss des Verfahrens vernichtet wurden. In 9 Prozent der Verfahren wurde ausdrücklich angeordnet, dass die Daten nicht vernichtet werden sollen. In den übrigen 88 Prozent der Verfahren ließen sich den Akten keine Hinweise hinsichtlich der Vernichtung der Daten entnehmen. Wenn die Daten vernichtet wurden, erfolgte dies entweder durch die Staatsanwaltschaft (vier Fälle) oder durch die Polizei (sieben Fälle).

2. Experteninterviews

Etwas weniger als die Hälfte der befragten Staatsanwälte gaben an, dass eine Vernichtung der Daten nach Abschluss des Verfahrens stattfände. Weiter wurde ausgeführt, dass dies einzelfallabhängig sei. Bei Verfahren gegen Unbekannt fände keine Vernichtung statt. Die Daten würde ggf. wieder gebraucht, wenn sich weitere Ermittlungsansätze ergeben. Ebenso würden die Daten nicht vernichtet, wenn sie zur Beweisführung in weiteren Verfahren benötigt würden. Gerade bei größeren Verfahren gebe es oftmals Schnittstellen zu anderen Verfahren bzw. anderen Verdächtigen. Zudem würden die Daten oft auch deshalb zurückgehalten, weil Verfahren (auch nach Erlass des Urteils) wieder aufgenommen werden könnten. Die Vernichtung sei daher die Ausnahme. Ein weiterer Befragter meint, dass hier die aus anderen Fällen bekannte Fehlerquelle wirke. Die Vernichtung der Daten unterbleibe keineswegs absichtlich. Aber wenn die Daten sich nicht in einem Sonderband befänden, sondern mitten in der Akte, dann könne man nicht ausschließen, dass die Löschung unterlassen wird. Das sei jedoch die Ausnahme. Es gebe keine gesonderte Statistik darüber wie bei der Telekommunikationsüberwachung nach § 100a

StPO. In der Regel gebe es aber ein Sonderheft, das nach Abschluss des Verfahrens vernichtet wird. Die Löschung werde dann in der Akte vermerkt. Dagegen gaben zwei Staatsanwälte an, dass die Daten nicht vernichtet werden. Sie würden in der Akte verbleiben und Aktenbestandteil werden. Ebenso verhalte es sich bei Disketten. Die Daten würden nicht vernichtet, da diese lediglich besagen, von welchem Anschluss aus eine Tat begangen wurde, führt einer der Befragten aus. Vier befragte Staatsanwälte geben an, dass sie nicht wüssten, ob die Daten vernichtet werden oder nicht. Sie gingen aber von der Löschung aus. Zudem gebe es normale Aktenvernichtungsfristen. Der Rechtspfleger beim Gericht betreue das weitere Verfahren.

3. Zusammenfassung der Ergebnisse

Nur in 3 Prozent der ausgewerteten Verfahren konnte den Akten explizit entnommen werden, dass die Verkehrsdaten vernichtet wurden. In 9 Prozent der Verfahren wurde ausdrücklich vermerkt, dass die Daten nicht vernichtet werden sollen und in 88 Prozent der Verfahren waren den Akten keine Hinweise hinsichtlich der Datenvernichtung zu entnehmen. Einschränkend ist zu bemerken, dass den Akten nicht entnommen werden konnte, ob ein ggf. existierendes Sonderheft mit Daten vernichtet wurde. Da jedoch gesetzlich vorgeschrieben ist, dass die Vernichtung der Daten in den Akten vermerkt sein muss (vgl. § 100h I Satz 3 i. V. m. § 100b VI Satz 2 StPO), ist davon auszugehen, dass die Daten in den Fällen, in denen sich keine Hinweise darauf ergaben, nicht vernichtet worden sein dürften. Auch die Expertengespräche unterstreichen diese Interpretation. Etwas weniger als die Hälfte der befragten Staatsanwälte gab zwar an, dass die Daten vernichtet würden. Die übrigen Staatsanwälte teilten freilich mit, dass die Daten nicht vernichtet würden bzw. dass nicht bekannt sei, ob eine Löschung stattfinde. Freilich fällt die Aufgabe der Löschung in den Aufgabenkreis der Staatsanwaltschaft.

XI. Verfahrensausgang

1. Verfahrensausgang allgemein

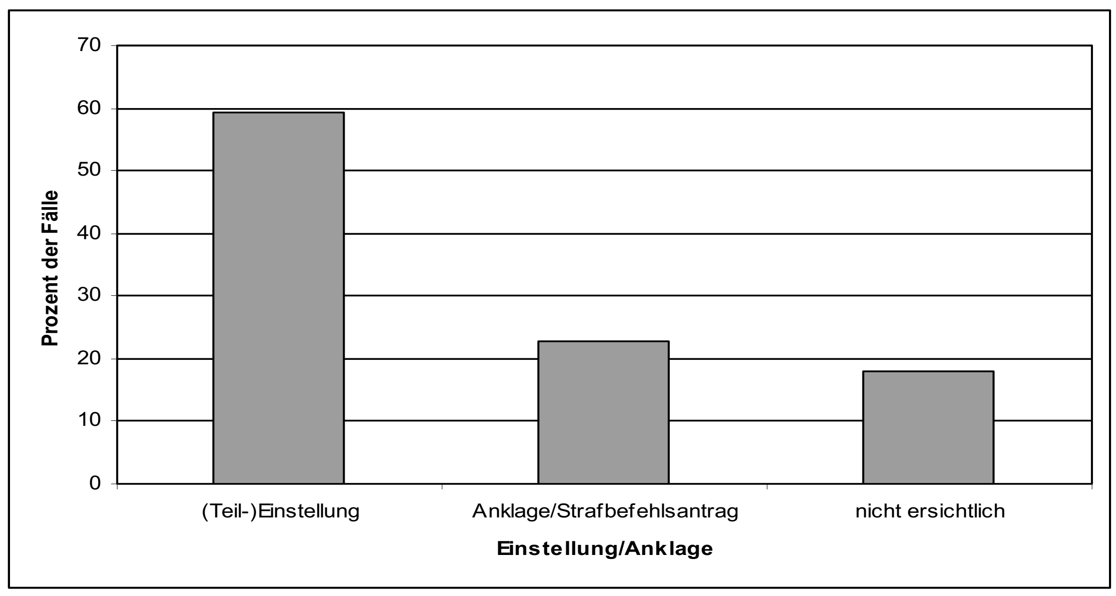
a) Anklage und Einstellung vor Anklageerhebung

In den 467 ausgewerteten Verfahren wurden 697 Beschuldigte ermittelt. Die Verfahren gegen die Beschuldigten sowie die Verfahren, in denen kein Beschuldigter identifiziert werden konnte, wurden überwiegend eingestellt (Abbildung 84).

In 58 Prozent der Fälle wurde das Verfahren vor Anklageerhebung eingestellt und in 1 Prozent der Fälle erfolgte eine Teileinstellung. Anklage wurde in 21 Prozent der Fälle erhoben und ein Strafbefehlsantrag wurde in 2 Prozent der Fälle gestellt. In 18 Prozent der Fälle war nicht ersichtlich, wie das Verfahren ausgegangen ist bzw. war das Verfahren noch nicht abgeschlossen. Zum großen Teil beruhte der Umstand, dass der Ausgang des Verfahrens nicht ersichtlich war, darauf, dass das Verfahren gegen den jeweiligen Beschuldigten abgetrennt worden war. Weiter kam es vor, dass es sich um Rechtshilfeersuchen handelte, bei denen ein anderes Land die Ermittlungen führte. Im Übrigen ließ sich den Akten der Ausgang des Verfahrens wegen der Unvollständigkeit der Akten nicht entnehmen.

Abbildung 84


Einstellung vor Anklageerhebung und Anklage (beschuldigtenbezogen)



b) Begründungen für die Einstellungen vor Anklageerhebung

Die Verfahren gegen die Beschuldigten wurden aus verschiedenen Gründen eingestellt. Welche Rechtsgrundlagen den Einstellungen zugrunde lagen, lässt sich Tabelle 21 entnehmen. Am häufigsten wurde das Verfahren gegen die Beschuldigten gemäß § 170 II StPO eingestellt (79 Prozent)[452]. In 4 Prozent der Fälle war kein eindeutiger Einstellungsvermerk in den Akten zu finden, aber es war ersichtlich, dass die Ermittlungen wegen Erfolglosigkeit nicht weiter geführt wurden, so dass von einer Einstellung auszugehen war. Bei je 3 Prozent der Einstellungen wurde das Verfahren gemäß § 153 I StPO wegen Geringfügigkeit und gemäß § 154 I StPO eingestellt. Im Übrigen erfolgten Einstellungen wegen des Verbots der Doppelverfolgung (Artikel 103 III GG, 2 Prozent), wegen § 45 JGG (bei Jugendlichen, 2 Prozent), wegen § 153a I StPO (1 Prozent) sowie wegen § 154b I StPO (1 Prozent). Zudem wurde das Verfahren vorläufig eingestellt wegen unbekannten Aufenthaltsorts des Beschuldigten (§ 205 StPO analog, 1 Prozent). Selten wurde auf den Privatklageweg (§§ 374 ff. StPO) verwiesen. Sonstige Einstellungen (z. B. § 31a BtMG) erfolgten bei 1 Prozent der Fälle.

Tabelle 21

Einstellungsgrundlagen

	N	Prozent der Beschuldigten
§ 170 II StPO	402	*78,8*
§ 153 I StPO	15	*2,9*
§ 154 I StPO	15	*2,9*
Einstellung wg. Verbot der Doppelverfolgung	11	*2,2*
§ 45 JGG	9	*1,8*
§ 153a I StPO	6	*1,2*
§ 154b I StPO	6	*1,2*
§ 205 StPO analog	6	*1,2*
Verweis auf Privatklageweg	3	*0,6*
Sonstiges	4	*0,8*
keine explizite Einstellung, aber naheliegend	20	*3,9*
RGL unbekannt	13	*2,5*
	510	***100,0***

Die Begründungen für die Einstellung des Verfahrens nach § 170 II StPO bezogen sich einerseits darauf, dass der Täter nicht ermittelt werden konnte (144) und andererseits darauf, dass kein Tatnachweis erbracht werden konnte (129).

Der Zusammenhang der eingestellten Verfahren mit der Abfrage der Verkehrsdaten lässt sich nicht genau bestimmen. Allgemein kann man jedoch sagen, dass in den Verfahren gegen die Beschuldigten, in denen die Verkehrsdatenabfrage als nicht erfolgreich oder nur bedingt erfolgreich eingestuft wurde, die häufigsten Einstellungen nach § 170 II StPO erfolgten. Bei nicht erfolgreicher Verkehrsdatenabfrage (dies betrifft 144 Beschuldigte) wurde das Verfahren gegen 76 Beschuldigte nach § 170 II StPO eingestellt, bei bedingt erfolgreicher Verkehrsdatenabfrage (dies betrifft 91 Beschuldigte) in 35 Fällen und bei erfolgreicher Verkehrsdatenabfrage (dies betrifft 93 Beschuldigte) nur in 14 Fällen. Ausführlicher wird diese Thematik noch einmal im Effizienzteil erörtert werden.

c) Verurteilung, Einstellung und Freispruch

In Abbildung 85 wird der Inhalt des Urteils bezogen auf die angeklagten Beschuldigten (211) zusammengefasst dargestellt.

Wenn Anklage erhoben wurde, wurden die Beschuldigten in 85 Prozent der Verfahren auch verurteilt. Teileinstellung (1 Prozent) und Teilfreispruch (1 Prozent) kamen selten vor. Im Übrigen erging in 6 Prozent der Fälle Freispruch und in 7 Prozent der Fälle wurde das Verfahren in der Hauptverhandlung eingestellt.

d) Verurteilungsinhalt

Wenn es nach Anklage zu einer Verurteilung kam, dann wurden zu 48 Prozent unbedingte Freiheitsstrafen verhängt (Abbildung 86).

In 36 Prozent der Verurteilungen wurden Bewährungsstrafen verhängt und bei 8,6 Prozent wurden die Angeklagten zu einer Geldstrafe verurteilt. Rechtsfolgen nach dem Jugendgerichtsgesetz waren ebenfalls zu beobachten. In 5,7 Prozent der Verfahren wurde eine Jugendstrafe ausgesprochen und zu je 0,6 Prozent wurden Jugendlichen oder Heranwachsenden Erziehungsmaßregeln oder Zuchtmittel auferlegt. Die Sanktionsstruktur spricht demnach dafür, dass ein bedeutsamer Anteil der Verfahren allenfalls der mittleren Kriminalität zuzuordnen ist. Bezieht man die Geringfügigkeitseinstellungen ein und rechnet Geldstrafen, Bewährungsstrafen[453] und Rechtsfolgen des JGG ohne Jugendstrafe zu diesem Kriminalitätsbereich, dann beziehen sich die Verfahren hierauf zu knapp 60 Prozent.

[452] In den Verfahren gegen unbekannte Täter (181 Verfahren) wurde das Verfahren in 91 Prozent der Fälle gemäß § 170 II StPO eingestellt. In den übrigen dieser Fälle war entweder keine explizite Einstellung ersichtlich oder das Verfahren wurde wegen des Verbots der Doppelverfolgung oder wegen Geringfügigkeit eingestellt.

[453] Das Bundesverfassungsgericht hat im Jahr 2003 ausdrücklich beanstandet, dass ein Fall, in welchem eine Freiheitsstrafe zur Bewährung ausgesetzt worden war, ohne weitere Prüfung als Straftat von erheblicher Bedeutung (i. S. v. § 81g StPO bzw. § 2 DNA-IfG) bewertet worden war; BVerfG, StV 2003, S. 1, 2.

Abbildung 85



Inhalt des Urteils

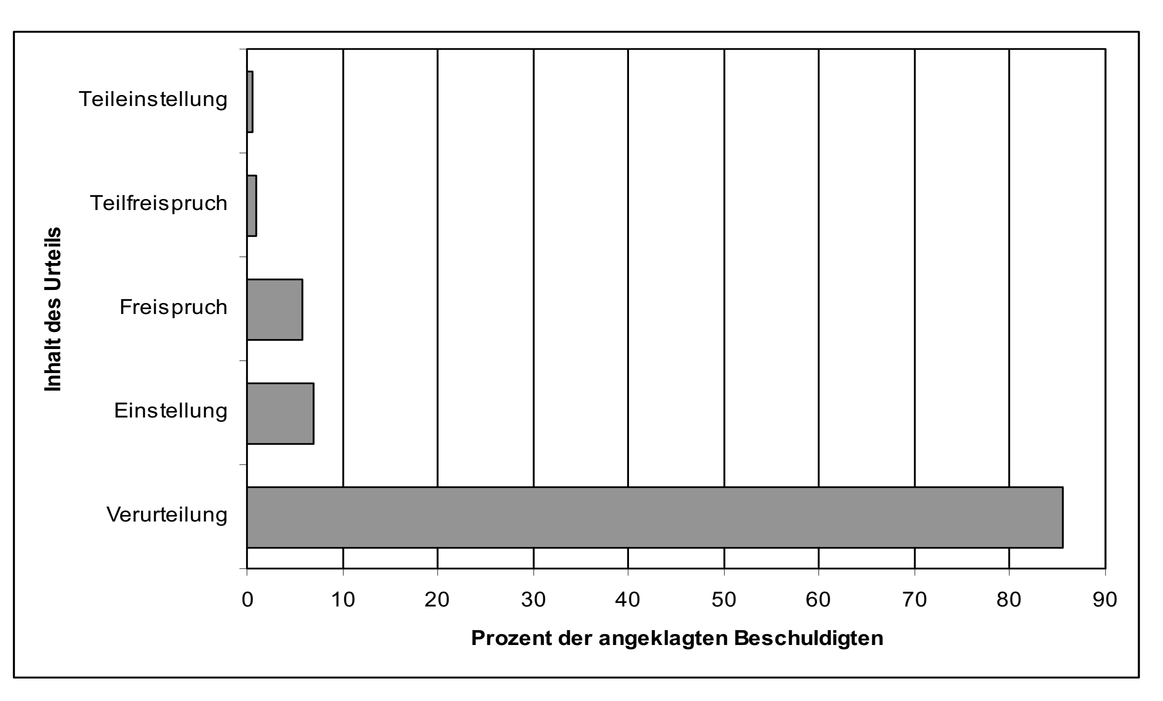
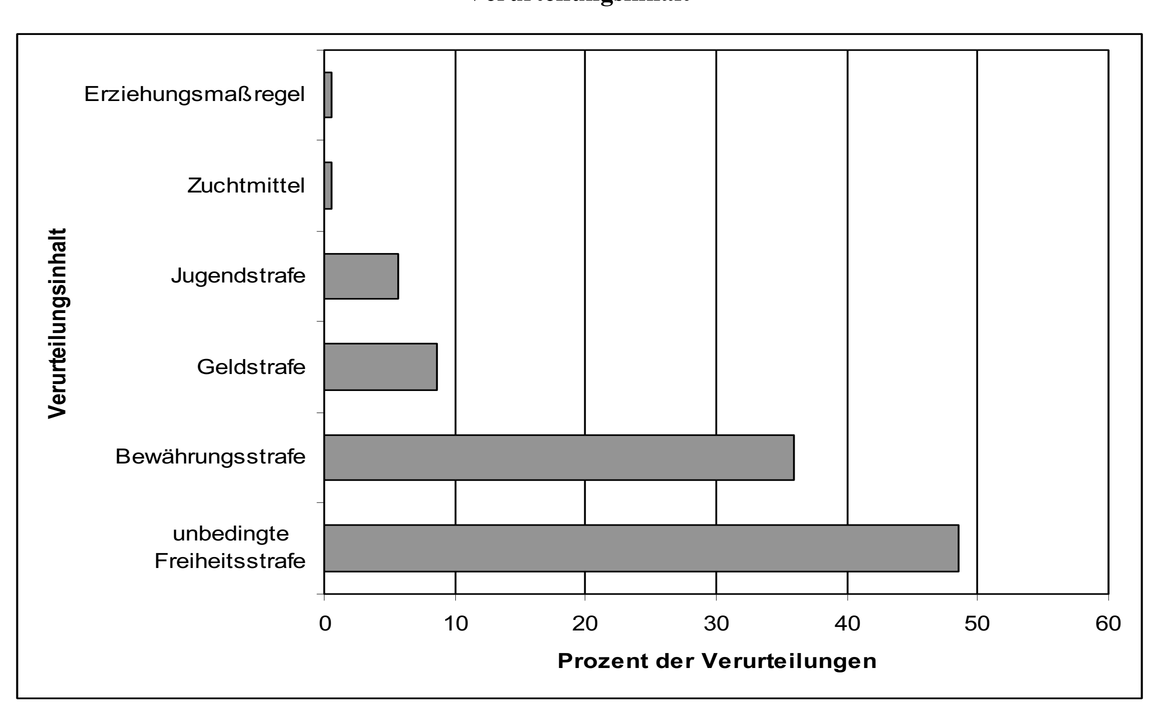


Abbildung 86

Verurteilungsinhalt



(1) Freiheitsstrafe

158 Angeklagte wurden zu einer Freiheitsstrafe mit oder ohne Bewährung verurteilt. Die Dauer der Freiheitsstrafen liegt zwischen einem Monat und 15 Jahren bzw. Lebenslänglich. Wie sich die Dauer der Freiheitsstrafen auf die Angeklagten verteilt, ergibt sich aus Abbildung 87. Freiheitsstrafen zwischen einem und zwei Jahren bilden mit etwa 45 Prozent die häufigste Ausprägung. In der Kategorie „über zehn Jahre“ sind im Übrigen auch die lebenslänglichen Freiheitsstrafen erfasst, die ein Drittel dieser Kategorie ausmachen.

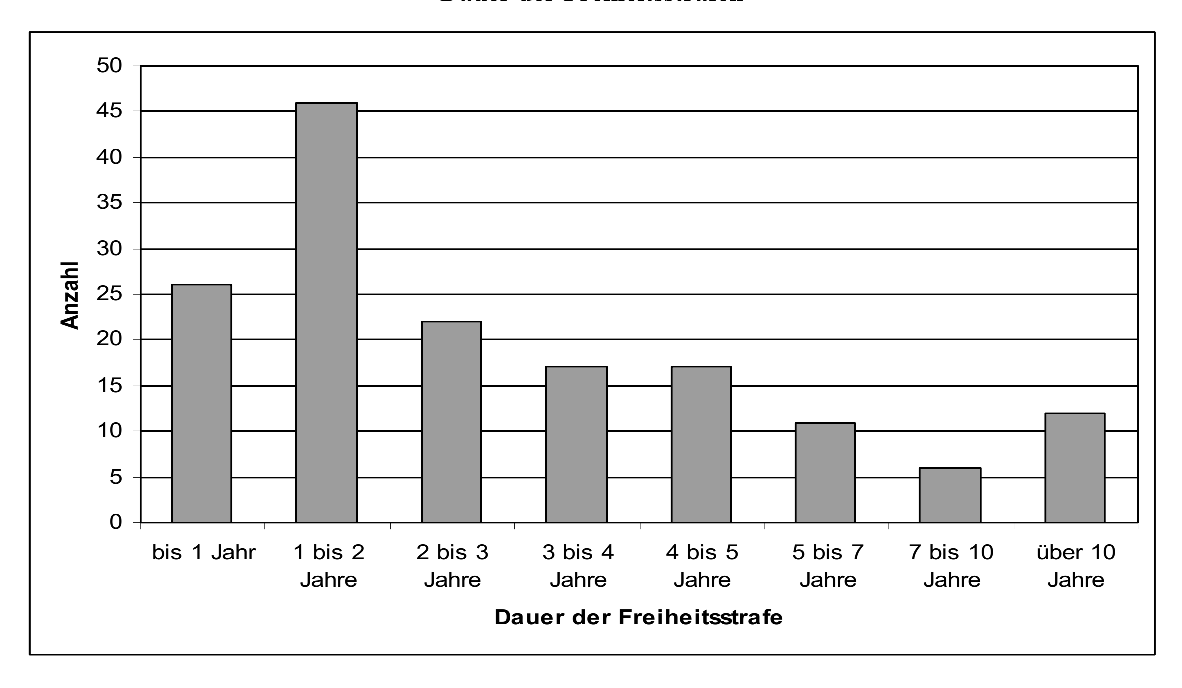
32 Verurteilten wurde mit der Aussetzung der Freiheitsstrafe zur Bewährung eine Auflage oder Weisung erteilt. In 17 Fällen kam es zur Anordnung einer Geldauflage. Die Höhe der Geldauflagen variierte zwischen 125 und 3 000 Euro. Arbeitsstunden wurden in Höhe von 30 bis zu 300 verhängt. Von den Arbeitsstunden waren acht Verurteilte betroffen. Die sonstigen Auflagen und Weisungen beinhalteten u. a. die Verpflichtung zur Teilnahme an einer Drogentherapie. Bei 49 Beschuldigten konnte den Akten die Festlegung der Bewährungszeit entnommen werden. Sie betrug in 61 Prozent der Fälle drei Jahre, in 27 Prozent zwei Jahre und in 12 Prozent vier Jahre.

(2) Geldstrafe

In 17 Fällen wurde eine Geldstrafe verhängt. Dabei wurden Geldstrafen von 120 bis 3 600 Euro zugemessen (Mittelwert 1 231 Euro). Die Tagessatzanzahl bewegte sich zwischen zehn und 90 Tagessätzen. Die Tagessatzhöhe belief sich auf 10 Euro bis 50 Euro.

Abbildung 87

Dauer der Freiheitsstrafen



2. Differenzierung nach Delikten

Zunächst erfolgte eine Betrachtung der bei den Beschuldigten aufgenommenen Delikte. Dabei wird wiederum zwischen Katalogdelikten und sonstigen Delikten unterschieden.

a) Katalogdelikte

Einstellung und Anklage (bzw. Strafbefehlsantrag) verteilen sich wie in Abbildung 88 dargestellt auf die Katalogdelikte des § 100a Satz 1 StPO. Daneben wird gezeigt, wie viele Verfahren gegen unbekannt geführt wurden und bei denen der Täter unbekannt blieb. Diese Verfahren wurden ebenfalls eingestellt und sind nicht in den übrigen Einstellungen enthalten.

Die absoluten Zahlen der Einstellungen sind bei Raub bzw. räuberischer Erpressung (53 Beschuldigte), bei (schweren) Bandendiebstählen (47) und bei Tötungsdelikten (28) recht hoch. Verfahren gegen Unbekannt konzentrieren sich auf den Raub. Die Anklagequoten verteilen sich wie folgt: Verfahren gegen die persönliche Freiheit (78 Prozent); Verfahren wegen Betäubungsmittelgesetz und gewerbsmäßiger Hehlerei (jeweils 65 Prozent) sowie Geldfälschung (55 Prozent). Bei den anderen Delikten liegt die Anklagequote unter 40 Prozent.

b) Sonstige Delikte

Bei den sonstigen Straftaten, also solchen, die nicht unter den Katalog des § 100a Satz 1 StPO fallen, ist zwischen den Delikten, die mittels Endeinrichtung begangen wurden (insgesamt 102), und denen, die ohne Endeinrichtung begangen wurden (insgesamt 253), zu unterscheiden. Auch hier sind die Verfahren gegen unbekannt wiederum separat aufgeführt. Die Straftaten, die mittels Endeinrichtung begangen wurden, sind in Abbildung 89 dargestellt.

Dabei fällt auf, dass sich Verfahren gegen Unbekannt auf den Betrug mittels Endeinrichtung konzentrieren (29). Auch bei der Androhung von Straftaten mittels Endeinrichtung liegen einige Verfahren gegen Unbekannt vor (8). Einstellungen sind häufig zu beobachten bei Beleidigungen mittels Endeinrichtung (17) und Straftaten gegen die persönliche Freiheit mittels Endeinrichtung (z. B. Bedrohung, Nötigung: 11). Einstellungen gegen Beschuldigte, die wegen spezieller Computerkriminalität verfolgt wurden (6) sowie bei sonstigen Straftaten mittels Endeinrichtung (7) sind ebenfalls hervorzuheben.

Die Nichtkatalogtaten, die *nicht* mittels Endeinrichtung begangen wurden, sind in Abbildung 90 dargestellt.

Verfahren gegen Unbekannt kamen besonders häufig bei schweren Diebstahlsdelikten (40) vor. Dort waren auch die Einstellungen am häufigsten (35). Häufig eingestellt wurde das Verfahren auch gegen Beschuldigte, die wegen einfachen Diebstahls (26), Betrugs (zwölf), sonstiger Straftaten (19), Hehlerei (12) und Betäubungsmitteldelikten (12), die nicht unter § 100a Satz 1 StPO fallen, verfolgt wurden. Anklagen konzentrieren sich auf den schweren Diebstahl (19), Betrug (15) und Körperverletzungsdelikte (13).

Abbildung 88


Anzahl Einstellungen und Anklagen differenziert nach Katalogdelikten

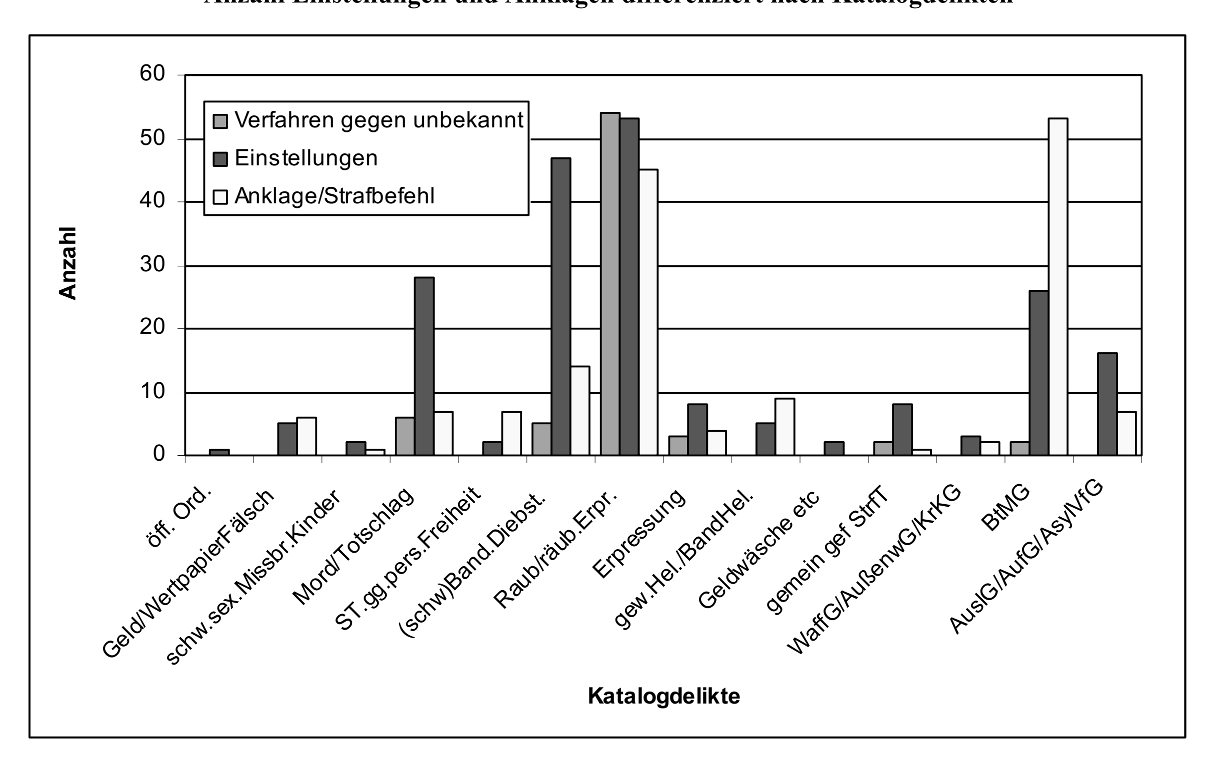


Abbildung 89

Anzahl Einstellungen und Anklagen differenziert nach sonstigen Straftaten mittels Endeinrichtung

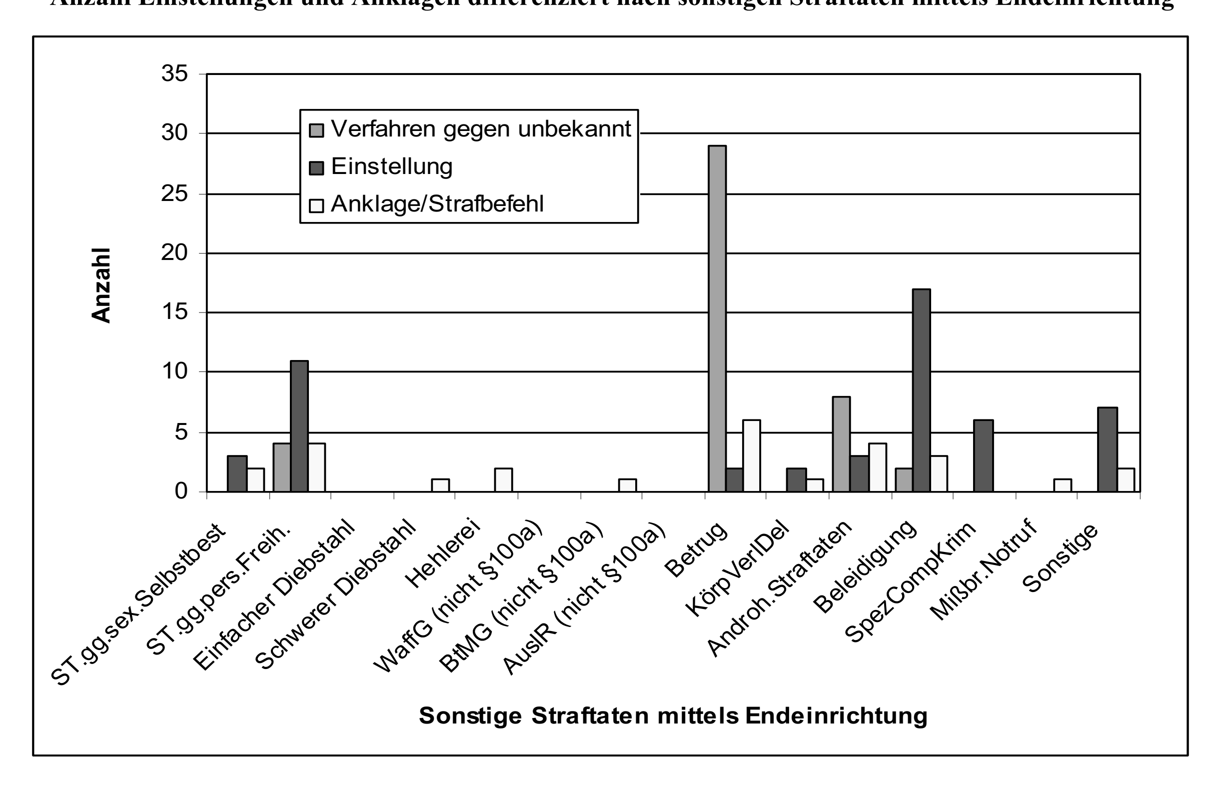
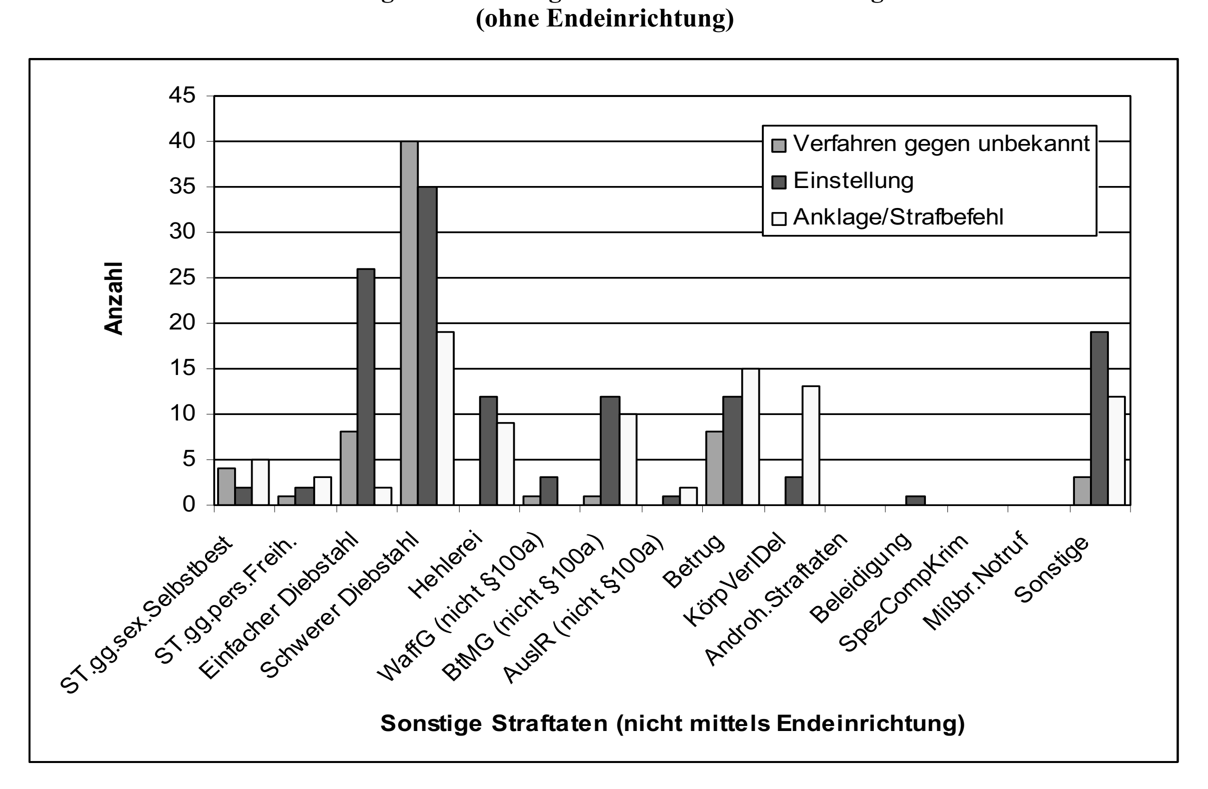


Abbildung 90

Anzahl Einstellungen und Anklagen differenziert nach sonstigen Straftaten (ohne Endeinrichtung)



3. Deliktsbezogene Betrachtung

Die bisherigen Betrachtungen bezogen sich auf die pro Beschuldigten notierten Ermittlungsdelikte (aus Tabelle „Beschuldigte“). Bei den folgenden Betrachtungen, insbesondere zu Anklage und Urteil, wurde auf die detaillierte Erfassung der Delikte in der „Anklage-Urteil-Delikts“-Tabelle zurückgegriffen, da nur hier auch die durch die Verurteilungen abgedeckten Delikte erfasst waren. Es kann dadurch zu minimalen Verschiebungen kommen, die aber die prinzipiellen Aussagen nicht tangieren. In den 467 Verfahren (davon 181 gegen unbekannt) wurden 211 Beschuldigte[454] wegen insgesamt 500 Delikten[455] angeklagt. Davon waren 232 Katalogdelikte und 268 sonstige Straftaten. Die Verurteilungen beziehen sich auf 186 Katalogdelikte und 204 sonstige Delikte.

a) Anklage und Einstellung bei Katalogdelikten

In Abbildung 91 ist dargestellt, wie sich Anklage und Einstellung auf die Katalogdelikte verteilen. Hierbei ist zu berücksichtigen, dass im Gegensatz zu den Ausführungen zu den Delikten, wegen derer die Ermittlungen eingeleitet wurden, nicht nur Mehrfachnennungen in Bezug auf verschiedene Delikte möglich waren, sondern auch Mehrfachnennungen einzelner Delikte vorhanden sein können, soweit sich diese in ihren spezifischen Begehungsweisen unterschieden. So kann dasselbe Delikt einmal vollendet und einmal im Versuch vorgelegen haben oder es kann z. B. zu unterschiedlichen Qualifikationen gekommen sein.

Die Anklagequote ist besonders stark ausgeprägt bei Betäubungsmitteldelikten, Straftaten gegen die persönliche Freiheit, Hehlerei und Fälschungsdelikten. Demgegenüber sind Anklagen und Einstellungen beim Raub ausgewogen. Sehr niedrig dagegen fällt die Anklagequote bei Tötungsdelikten aus.

b) Anklage und Einstellung bei sonstigen Delikten

Abbildung 92 zeigt die Verteilung von Anklagen und Einstellungen bei den einzelnen Delikten, die nicht unter den Katalog des § 100a Satz 1 StPO fallen. Häufig angeklagt wurden Körperverletzungsdelikte, Betrugsdelikte, Betäubungsmitteldelikte und schwere Diebstahlsdelikte. Bei letzteren sind allerdings auch die meisten Einstellungen zu verzeichnen. Am häufigsten wurde wegen sonstiger Delikte angeklagt. Dabei handelt es sich u. a. um Verstöße gegen die Abgabenordnung (Steuerstraftaten, Steuerhinterziehung, Steuerhehlerei, Schmuggel, 26), Urkundenfälschungen (17), Fahren ohne Fahrerlaubnis (9), Verschaffen von falschen amtlichen Ausweisen (6), Inverkehrbringen von Falschgeld (6), Vortäuschen von Straftaten (5) und Unterschlagung (5). Bei diesen Delikten wurde das Verfahren aber auch oft eingestellt. Häufige Einstellungen erfolgten zudem bei Betäubungsmitteldelikten und einfachem Diebstahl.

[454] Dabei ist zu berücksichtigen, dass der Verfahrensausgang bei 157 Beschuldigten wegen Abtrennung des Verfahrens oder anderen Gründen nicht bekannt ist. Die Verfahren wurden gegen 510 Personen eingestellt.

[455] In dieser Zählung wurden jeweils Fälle gleichen Delikts und gleicher Begehungsweise pro Beschuldigten nur einmal gezählt.

Abbildung 91



Anklage und Einstellung bei Katalogdelikten (deliktsbezogen)

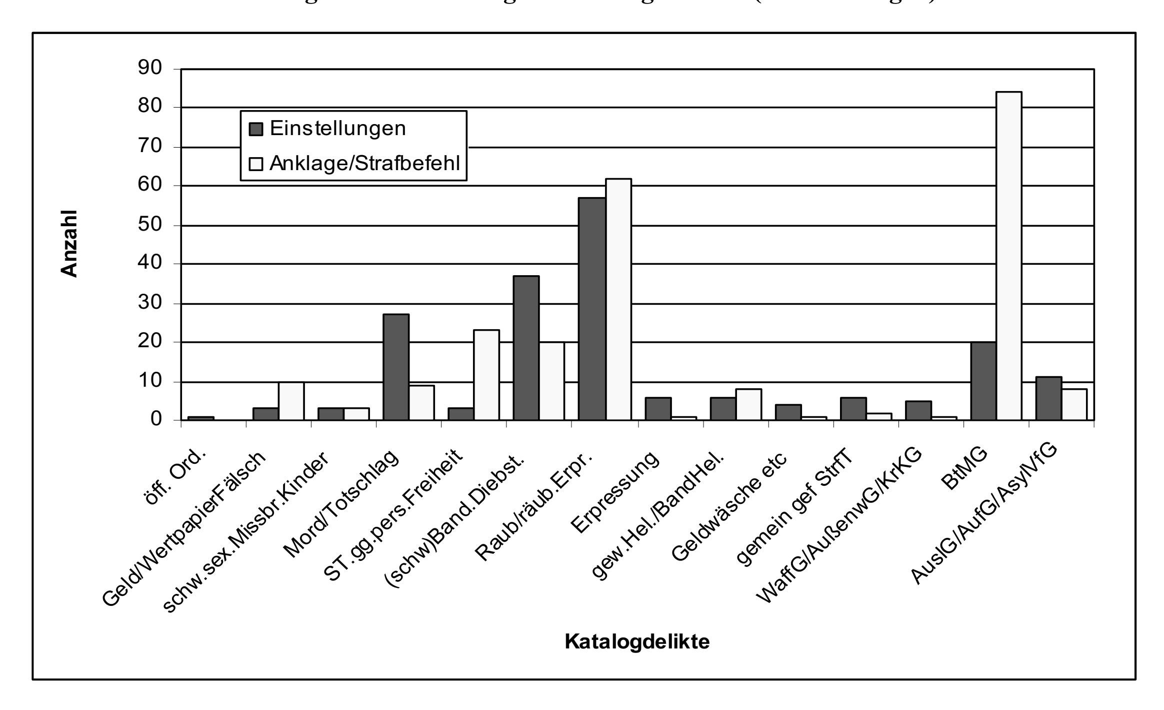
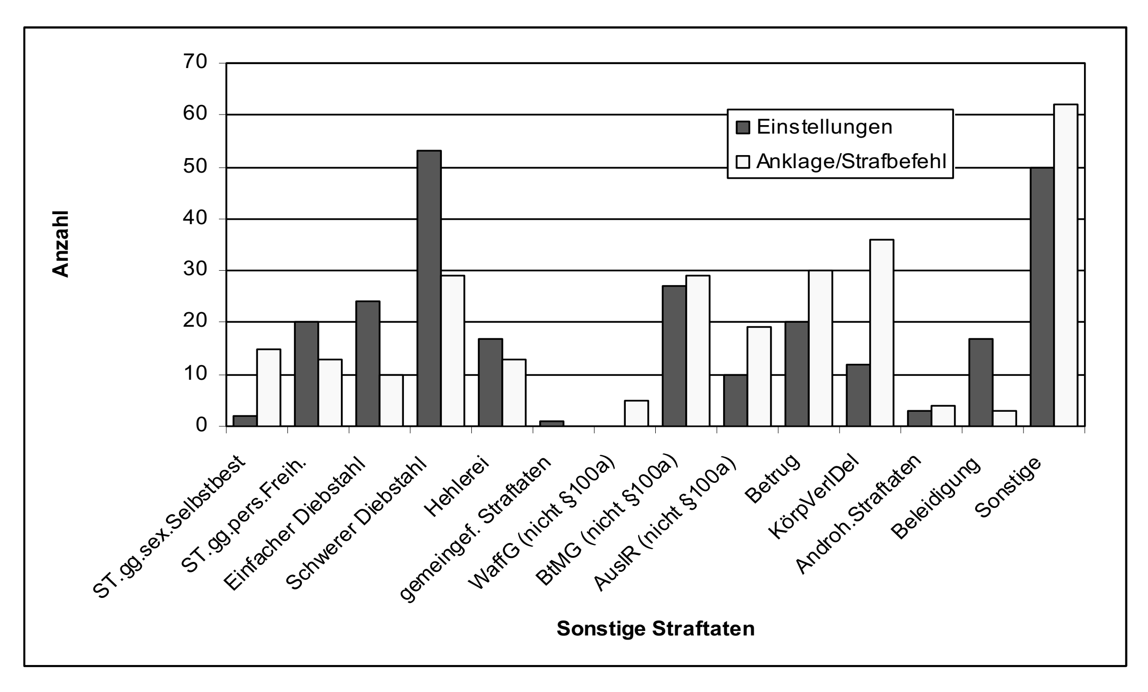




Abbildung 92

Anklage und Einstellung bei sonstigen Delikten (deliktsbezogen)



c) Verurteilungen bei Katalogdelikten

Im Folgenden wird dargestellt, in welcher Relation Anklage und Verurteilung zueinander stehen. Abbildung 93 gibt wieder, wie viele Katalogdelikte jeweils angeklagt wurden und welcher Prozentsatz davon auch verurteilt wurde. Zusätzlich ist die Anzahl der zunächst nicht angeklagten, aber im Urteil erscheinenden Katalogdelikte angegeben.

Die häufigsten angeklagten Katalogdelikte sind Betäubungsmitteldelikte. Sie zeichnen sich durch eine relativ hohe Verurteilungsquote (80 Prozent) aus. Sehr häufig wurden auch Raub und räuberische Erpressung angeklagt. Bei diesen Delikten wurde zu 87 Prozent verurteilt. Zu 100 Prozent wurden schwerer sexueller Missbrauch von Kindern, Totschlagsdelikte, Erpressung, gemeingefährliche Straftaten, Straftaten nach dem Waffengesetz sowie Verstöße gegen Vorschriften des Ausländerrechts verurteilt, wobei jedoch zu beachten ist, dass hier nur wenige Fälle angeklagt waren und damit die Bestimmung der Verurteilungsrate nicht allzu aussagekräftig ist. Dies gilt im verstärkten Maße auch bei der Geldwäsche, bei der nur ein Fall angeklagt war. Eine geringere Verurteilungsquote ist beim (schweren) Bandendiebstahl zu verzeichnen (50 Prozent). Unter den Delikten, die zunächst nicht angeklagt waren, wegen denen aber später verurteilt wurde, sind (schwerer) Bandendiebstahl und Erpressung etwas häufiger. Hier kann es sein, dass die Begehungsform eines Delikts im Laufe der Hauptverhandlung anders beurteilt wurde. So kann z. B. eine angeklagte räuberische Erpressung „nur“ als eine Erpressung verurteilt werden.

d) Verurteilungen bei sonstigen Delikten

In Abbildung 94 wird dargestellt, wie sich Anklage und Verurteilung auf Nichtkatalogtaten verteilen.

Am häufigsten angeklagt sind die bereits aufgeführten sonstigen Delikte. Verurteilt wurden diese Delikte zu 76 Prozent. Häufig angeklagte Delikte sind auch Körperverletzungsdelikte. Diese wurden zu 81 Prozent verurteilt. Betrugsdelikte sind ebenfalls häufig angeklagt und wurden zu 77 Prozent verurteilt. Betäubungsmitteldelikte, die nicht unter den Katalog des § 100a Satz 1 StPO fallen, werden häufig angeklagt und die Verurteilungsquote ist mit 97 Prozent sehr hoch. Schwerer Diebstahl wird zwar häufig angeklagt, wird aber nur zu 55 Prozent verurteilt. Besonders hohe Verurteilungsraten sind bei Straftaten gegen die sexuelle Selbstbestimmung, einfachem Diebstahl und bei der Androhung von Straftaten festzustellen, wobei die Zahl der angeklagten Delikte bei diesen eher gering ist. Der schwere Diebstahl ist das am häufigsten verurteilte Delikt, das nicht in der Anklageschrift aufgeführt war.

Abbildung 93



Anklage und Verurteilung bei Katalogdelikten (deliktsbezogen)

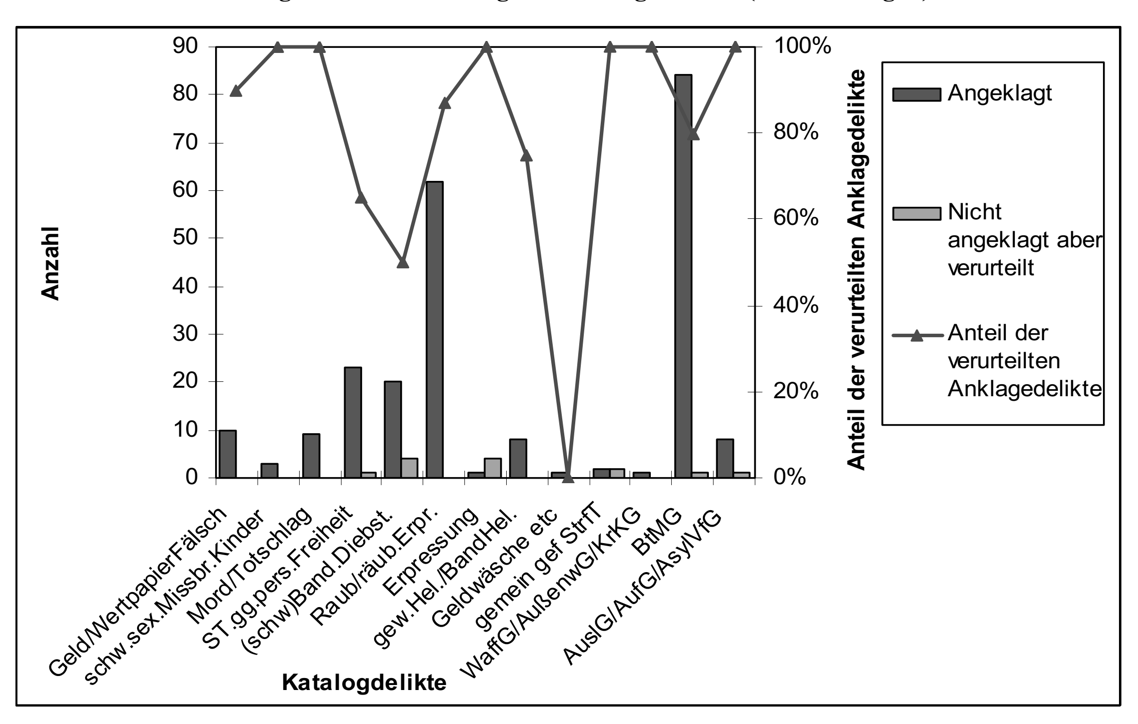
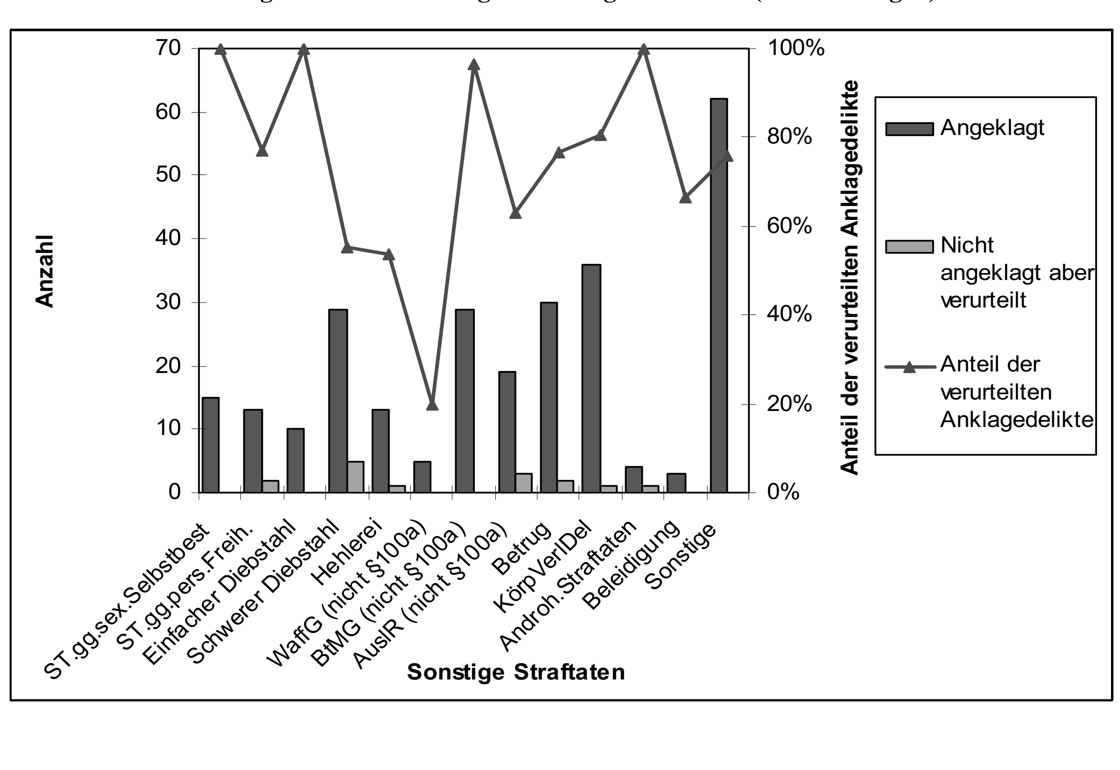


Abbildung 94

Anklage und Verurteilung bei sonstigen Delikten (deliktsbezogen)



4. Fallzahlen differenziert nach Delikten

Neben den Delikten selbst wurden auch die konkreten Fallzahlen, das heißt, die Zahl der Einzeltaten, die Einstellungen und Anklagen zugrunde lagen, erfasst. Welche Fallzahlen bei den einzelnen Katalogdelikten angeklagt wurden oder der Einstellung zugrunde lagen, lässt sich Abbildung 95 entnehmen.

Die höchsten Fallzahlen bei den Katalogdelikten waren bei (schweren) Bandendiebstählen (1 650) und Betäubungsmitteldelikten (985) zu verzeichnen. Dabei wurde bei ersteren besonders häufig eingestellt (1 553) und bei letzteren besonders häufig angeklagt (963). Für Rauschgiftdelikte ist charakteristisch, dass es sich nicht um Einzeltaten handelt, sondern dass sich gewerbsmäßige Geschäftsstrukturen entwickeln und daher immer wieder über mehrere Monate hinweg Geschäfte abgewickelt werden. Dadurch steigen die Fallzahlen in die Höhe. Bei Bandendiebstählen handelt es sich schon per Definition um eine Gruppe von Personen, die sich für einen längeren Zeitraum zur Begehung von Diebstählen zusammengeschlossen hat. Daher ist es auch hier typisch, dass die Beschuldigten wegen mehrerer Delikte angeklagt werden. Hohe Fallzahlen sind auch bei angeklagten Geld- und Wertpapierfälschung und bei angeklagten Verstößen gegen Vorschriften des Ausländerrechts zu verzeichnen. Hohe Fallzahlen bei eingestellten Delikten sind bei gewerbsmäßiger Hehlerei bzw. Bandenhehlerei und bei schwerem sexuellen Missbrauch von Kindern zu bemerken. Geringe Fallzahlen fallen bei Erpressung, Geldwäsche, gemeingefährlichen Straftaten, Verstößen gegen das Waffengesetz und Verstößen gegen die öffentliche Ordnung auf. Im Gegensatz zu schweren Bandendiebstählen oder Betäubungsmitteldelikten handelt es sich dabei aber auch nicht um typische Delikte, die wiederholt über einen längeren Zeitraum begangen werden.

Abbildung 96 stellt die Fallzahlen der sonstigen Straftaten dar, die Einstellung und Anklage zugrunde lagen.

Die höchsten Fallzahlen sind dabei bei schweren Diebstahlsdelikten (883) und bei sonstigen Delikten (1092) festzustellen. Es ist nicht unüblich für Wohnungseinbruchsdiebstähle, dass es sich dabei um eine Serie von Straftaten handelt und dadurch die Fallzahlen höher sind als bei anderen Delikten. Sowohl bei den schweren Diebstahlsdelikten als auch bei den sonstigen Delikten ist der Anteil an eingestellten Delikten sehr groß. Häufig angeklagt wurde wegen Betäubungsmitteldelikten, die nicht unter den Katalog des § 100a Satz 1 StPO fallen. Auch Betrugsdelikte und Verstöße gegen das Ausländerrecht weisen relativ hohe Fallzahlen auf. Dies lässt sich damit erklären, dass es sich z. B. beim Enkeltrick, der unter die Deliktskategorie Betrug fällt, typischerweise nicht um eine Einzeltat handelt, sondern um mehrere gleichartige Fälle, die in einem Verfahren verfolgt werden. Auch z. B. Schleusungen von Ausländern werden in der Regel gewerbsmäßig ausgeführt.

In Abbildung 97 werden die konkreten Fallzahlen zu den Katalogdelikten, welche in den Anklageschriften und in den Urteilen aufgeführt wurden, dargestellt.

Abbildung 95

Fallzahlen bei Anklage und Einstellung differenziert nach Katalogdelikten

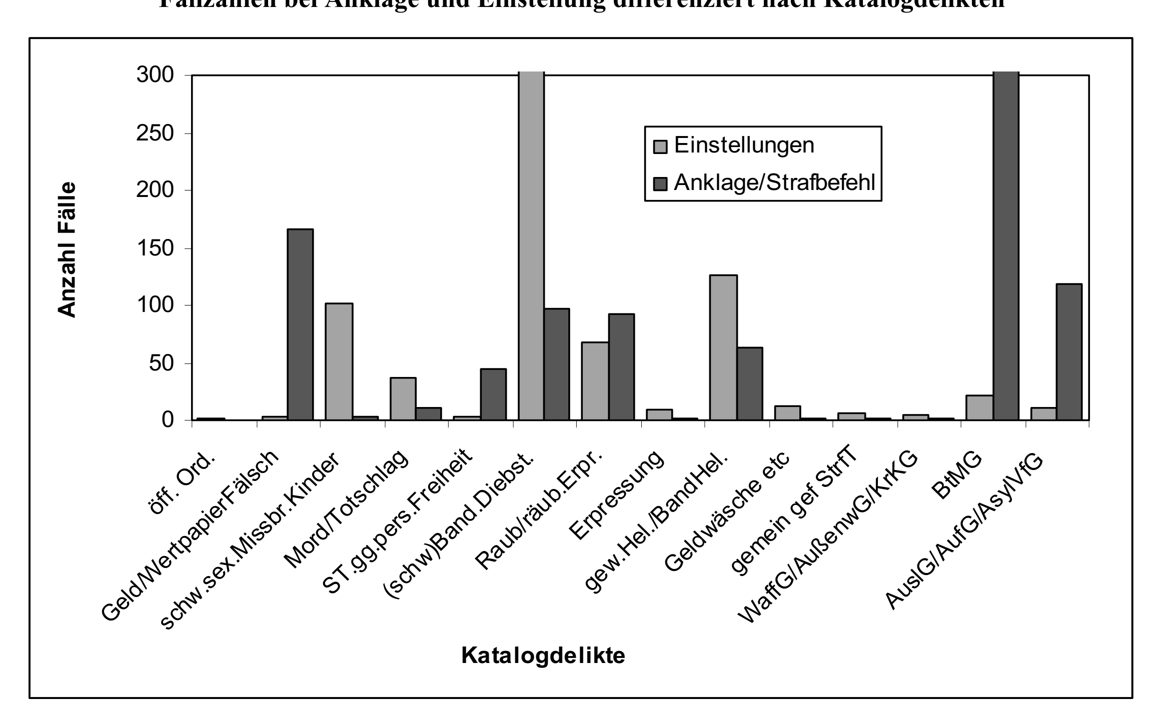




Abbildung 96

Fallzahlen bei Anklage und Einstellung differenziert nach sonstigen Delikten

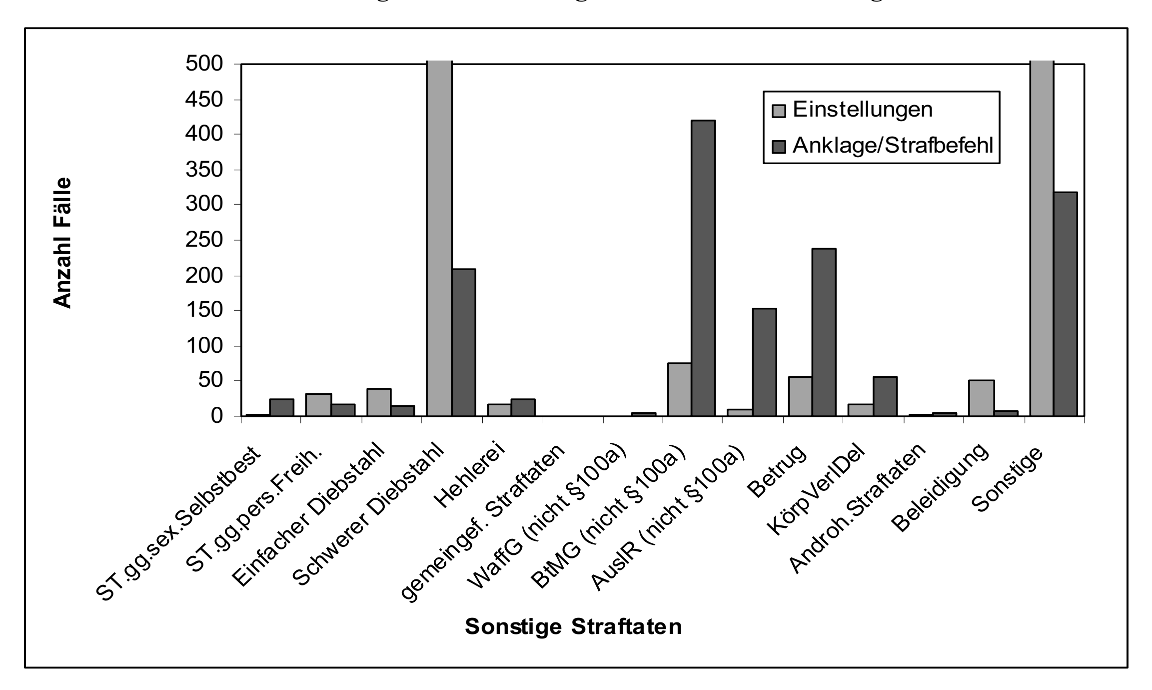
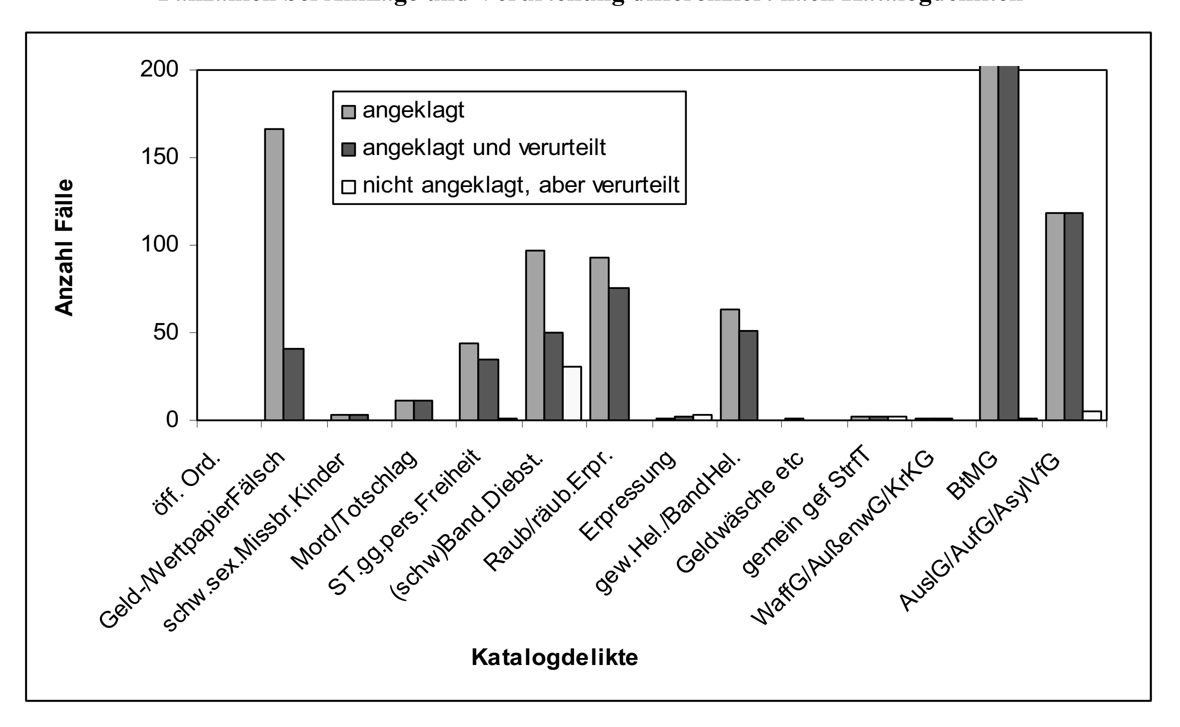


Abbildung 97

Fallzahlen bei Anklage und Verurteilung differenziert nach Katalogdelikten

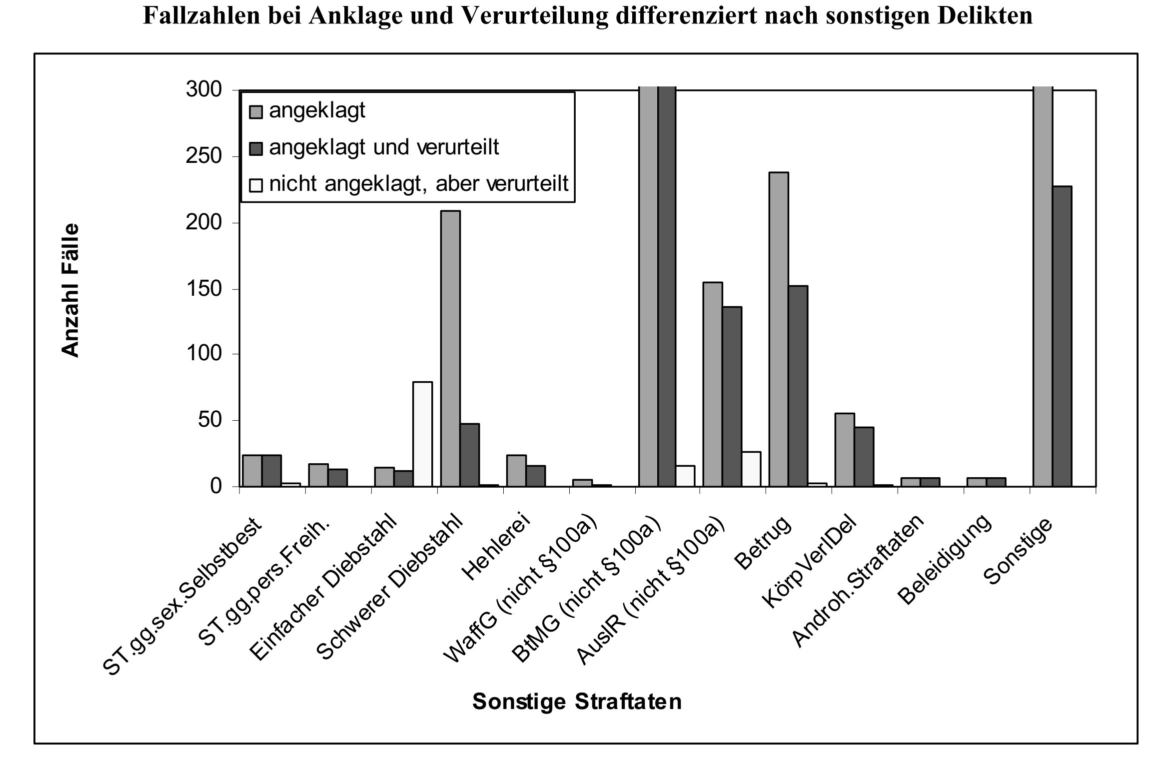


Von den häufig angeklagten Fällen von Betäubungsmitteldelikten (963) wurden nur etwa ein Drittel (383) verurteilt. Das kann darauf beruhen, dass die Vielzahl der Rauschgiftgeschäfte nicht konkret nachgewiesen werden kann und die Fallzahl daher im Urteil auf die nachweisbaren Drogengeschäfte reduziert wird. Auffällig ist auch die geringe Anzahl von verurteilten Fällen (41) bei der Geld- und Wertpapierfälschung (angeklagt: 166). Hier kann die Verurteilung ebenfalls an der Nachweisbarkeit scheitern. Beim schweren Bandendiebstahl wird nur etwa die Hälfte der angeklagten Fälle später verurteilt. Hier fällt auch die relativ hohe Anzahl von nicht in der Anklageschrift, aber im Urteil vorkommenden Delikten auf. Letzteres kann darauf beruhen, dass sich die Bewertung als Bandendiebstahl oder die Gewerbsmäßigkeit des Vorgehens erst in der Hauptverhandlung ergeben hat.

Abbildung 98 lässt sich entnehmen, wie sich die Fallzahlen der Straftaten, die nicht unter den Katalog des § 100a Satz 1 StPO fallen, auf Anklage und Urteil verteilen. Häufige Anklagen und Verurteilungen sind bei Betäubungsmitteldelikten und sonstigen Delikten zu bemerken. Auffällig ist die geringe Fallzahl verurteilter schwerer Diebstahlsdelikte und das häufige Vorkommen von nicht angeklagten, aber verurteilten einfachen Diebstählen. Hier kann sich jedoch die Einschätzung der Qualität des Diebstahls im Laufe der Hauptverhandlung verändert haben.

Abbildung 98

Fallzahlen bei Anklage und Verurteilung differenziert nach sonstigen Delikten



5. Zusammenfassung der Ergebnisse

Die im Rahmen der Aktenanalyse ausgewerteten Verfahren wurden überwiegend eingestellt. In 181 von 467 Verfahren (fast 40 Prozent der Verfahren) blieben die Täter unbekannt. Nur gegen 211 der 697 identifizierten Beschuldigten konnte Anklage erhoben werden. Insgesamt wurden 58 Prozent der Verfahren gegen die identifizierten Beschuldigten und gegen Unbekannt eingestellt und in 23 Prozent konnte Anklage bzw. Strafbefehlsantrag erhoben werden. In 18 Prozent der Fälle konnte der Ausgang des Verfahrens nicht ermittelt werden. Die Einstellungen wurden größtenteils auf der Grundlage des § 170 II StPO vorgenommen (79 Prozent der Fälle). Wenn Anklage erhoben wurde, konnten die Beschuldigten zu 87 Prozent verurteilt werden. Freigesprochen wurden die angeklagten Verurteilten zu 6 Prozent und nach Anklageerhebung eingestellt wurde das Verfahren in 7 Prozent der Fälle. In 36 Prozent der Verurteilungen wurde eine Freiheitsstrafe ohne Bewährung verhängt und damit eine Strafe, die eine gewisse Schwere der Taten indiziert. Die Einstellungs- und Sanktionsstruktur spricht im Übrigen dafür, dass sich die Straftaten in Verfahren mit Verkehrsdatenabfrage überwiegend in dem Bereich bis zu mittelschwerer Kriminalität bewegen.

Deliktsbezogen betrachtet liegt die Anklagequote bei Betäubungsmitteldelikten, die unter den Katalog des § 100a Satz 1 StPO fallen, am höchsten. Hier fiel mit 80 Prozent auch die Verurteilungsquote hoch aus. Die Anklagequoten sind weniger stark ausgeprägt bei Raub und räuberische Erpressung, hier ist der Anteil an Einstellungen vor Anklageerhebung recht hoch. Wenn diese Delikte jedoch angeklagt wurden, kam es in 87 Prozent der Fälle zu einer Verurteilung. Bei den Nichtkatalogtaten wurde häufig eingestellt, wenn besonders schwere Fälle des Diebstahls vorlagen. Häufige Anklagen gab es wegen Betrugsdelikten und Körperverletzungsdelikten. Bei beiden Delikten sind auch hohe Verurteilungsraten zu verzeichnen.

Dabei ist zu berücksichtigen, dass die Einstellungsquote von Verfahren generell sehr hoch ist. Da den ausgewerteten Verfahren ein breites Deliktsspektrum zugrunde liegt, können die Zahlen mit der allgemeinen Erledigungsstatistik verglichen werden.[456] Im Jahr 2003 wurde von insgesamt 4 766 070 erledigten Verfahren in 573 345 Fällen Anklage erhoben und in 603 999 Fällen Strafbefehl beantragt. Allein gemäß § 170 II StPO wurden 1 273 673 Verfahren eingestellt. Weitere 265 909 Verfahren wurden mit einer Auflage und 998 845 Verfahren ohne Auflage eingestellt.

XII. Rechtsbehelfe

1. Aktenanalyse

177 Beschuldigte wurden verurteilt. In 15 Fällen handelte es sich um Strafbefehle. Gegen die Urteile wurden in etwa 30 Prozent Rechtsmittel eingelegt. Davon entfallen etwa 60 Prozent auf eine Revision und 25 Prozent auf eine Berufung. Der Rest betrifft Einsprüche gegen einen Strafbefehl. In 32 Fällen ging es um eine Revision und in 14 Fällen um eine Berufung. Einspruch gegen einen Strafbefehl erfolgte in vier Fällen. Die Einlegung der Rechtsbehelfe erfolgte ganz überwiegend durch den Verurteilten (44 Fälle). Seitens des Opfers wurde in fünf Fällen ein Rechtsmittel eingelegt. Einen Bezug zur Verkehrsdatenabfrage konnte nur für eine Revision hergestellt werden. Der Verteidiger des Verurteilten erklärte in der Rechtsmittelbegründung, dass es sich bei den Daten nur um Indizien handele. Die Daten würden nicht nachweisen, wo sich der Verurteilte aufgehalten habe, sondern nur, wo sich das Mobiltelefon befand. Mit diesem könnte aber auch eine andere Person telefoniert haben. Die Revision wurde jedoch als unbegründet verworfen. Die nicht zurückgenommenen Rechtsbehelfe (38) wurden größtenteils verworfen (29). Im Übrigen führte die Einlegung der Rechtsmittel zur Abänderung in fünf Fällen und zur Aufhebung des Urteils in drei Fällen. Ein Zusammenhang der Verkehrsdatenabfrage mit der Abänderung oder Aufhebung des Urteils konnte in keinem Fall festgestellt werden.

2. Experteninterviews

Nur einer der befragten Verteidiger hat im Jahr 2005 Beschwerden gegen Maßnahmen nach §§ 100g, 100h StPO eingelegt, nachdem der Verwertung widersprochen worden war. Begründet sei dies aufgrund der Fehlerhaftigkeit der Beschlüsse gewesen. Weder sei ein Anordnungsgrund angegeben, noch Subsidiarität oder Verhältnismäßigkeit begründet worden. Keiner der Befragten hat im Jahr 2005 eine Berufung oder Revision im Zusammenhang mit Verkehrsdatenabfrage eingelegt. Einer der Befragten gab jedoch an, in 2006 eine Revision wegen seiner Meinung nach unverwertbaren Verkehrsdaten eingelegt zu haben. Ein anderer erklärte, dass in den Fällen, in denen die Verhältnismäßigkeit und die Verwertbarkeit problematisch waren, die Daten nicht als Beweismittel eingeführt worden seien. Zwei weitere Befragte gaben an, eine Berufung bzw. Revision eingelegt zu haben, wobei aber nicht Verstöße gegen Voraussetzungen der §§ 100g, 100h StPO, sondern solche wegen §§ 100a, 100b StPO tragend gewesen seien.

3. Zusammenfassung der Ergebnisse

In den ausgewerteten Verfahren wurde in 55 Fällen Rechtsmittel gegen Verurteilungen eingelegt. Dabei handelte es sich vor allem um Revisionen (32). Einen Bezug zur Verkehrsdatenabfrage gab es nur bei einer Revision, die jedoch keinen Erfolg hatte. Der Verteidiger wies dabei darauf hin, dass es sich bei den Daten nur um Indizien und nicht um Beweise handle. Die Rechtsmittel waren ganz überwiegend erfolglos. Dies deckt sich mit Befunden zu den Folgen von Rechtsmitteln im Allgemeinen. Die Expertengespräche mit den Verteidigern bestätigen dieses Bild. Nur ein einziges Verfahren wurde berichtet, in dem die Verkehrsdatenabfrage für die Begründung eines Rechtsmittels eine bedeutsame Rolle spielte.

---

[456] Statistisches Bundesamt (Hrsg.): Rechtspflege, Fachserie 10/Reihe 2.6: Staatsanwaltschaften 2003, Wiesbaden 2004.

XIII. Schwierigkeiten bei der Anwendung der Normen, Veränderungen gegenüber § 12 FAG und zukünftige Gestaltung der Maßnahme

Fragen danach, zu welchen Problemen es bei der Anwendung der §§ 100g, 100h StPO kommt, welche Veränderungen sich gegenüber der Regelung in § 12 FAG ergeben haben und wie die Beteiligten sich die Maßnahme zukünftig vorstellen, wurde mit den Befragungen und Interviews untersucht.

1. Schriftliche Befragung

a) Veränderungen gegenüber der Regelung in § 12 FAG

Die Frage, ob sich durch die Regelung der Auskunftserteilung über Verbindungsdaten in §§ 100g, 100h StPO gegenüber der alten Rechtslage, also der Regelung des § 12 FAG, Änderungen für die Praxis ergeben haben, beantworteten 65 Prozent mit Nein. Von denen, die die Frage bejahten, waren 68 Prozent der Ansicht, dass es seit der Änderung eine höhere Anzahl an Anordnungen gebe, wogegen 12 Prozent eine geringere Anzahl feststellten. Weiter gab etwa ein Drittel dieser Befragten (33 Prozent) an, dass nach der Änderung mehr Erfolge zu verzeichnen seien, 4 Prozent verbanden die Änderungen mit geringeren Erfolgen. Als weitere Änderungen in der Praxis nannten 28 Befragte folgende Aspekte: Die jetzige Regelung sei zu kompliziert und verursache einen höheren Aufwand. Im Gegensatz dazu wurde die jetzige Rechtslage von einigen Befragten auch als klarer und präziser bezeichnet. Eine weitere angesprochene Veränderung betrifft die Zugriffsmöglichkeit auf zukünftig anfallende Daten.

b) Auskunft über Personendaten zu dynamischen IP-Adressen

Die Staatsanwälte wurden danach gefragt, auf welcher Rechtsgrundlage Personendaten zu dynamischen IP-Adressen eingeholt werden. Darauf antworteten 53 Prozent mit §§ 100g, 100h StPO und 24 Prozent mit § 113 TKG. Andere Antworten bezogen sich auf die allgemeine Angabe des „TKG“ und § 161a StPO (jeweils 6 Prozent). 4 Prozent der Befragten teilten mit, dass sie teilweise §§ 100g, 100h StPO und teilweise § 113 TKG als Rechtsgrundlage heranzögen. 3 Prozent der Befragten führten aus, dass sie früher (im Jahr 2005) nach §§ 100g, 100h StPO vorgegangen seien, mittlerweile aber wegen der Rechtsprechung nach § 113 TKG vorgehen. Weitere 2 Prozent erklärten, dass sie nur deshalb §§ 100g, 100h StPO als Rechtsgrundlage wählten, da die Provider sich ohne Beschluss weigern würden und sich so Verzögerungen oder Beweisverluste vermeiden ließen. Weitere genannte Rechtsgrundlagen sind § 3 Nr. 3 TKG, §§ 89, 90 TKG, § 111 TKG, § 112 TKG, §§ 101, 101a StPO, § 161 StPO.

Die Frage, ob es dabei Schwierigkeiten gegeben habe, beantworteten 384 Befragte, wobei 67 Prozent sie verneinten und 33 Prozent zustimmten. Letztere führten zur Erklärung aus, dass von Betreiberseite Beschlüsse nach §§ 100g, 100h StPO verlangt würden (61 Prozent dieser Befragten). 12 Prozent berichteten, dass Anbieter sich geweigert hätten, die Maßnahme durchzuführen. Von 18 Prozent wurde als Problem die unterschiedliche Rechtsauffassung der Staatsanwaltschaften und der Provider angeführt. 11 Prozent gaben an, dass die Daten nicht mehr gespeichert gewesen wären. Als problematisch wurde auch die uneinheitliche Rechtsprechung zur Rechtsgrundlage für Personendatenauskünfte empfunden (7 Prozent). Weiter wurde angegeben, dass diese Problematik gesetzlich nicht klar geregelt sei. Ausgeführt wurde zudem, dass teilweise vorbeugend ein Beschluss beantragt werde, um Probleme mit den Anbietern zu vermeiden.

c) Hinreichende Bestimmung des Betroffenen

Die Vorschrift des § 100h I Satz 1 StPO sieht vor, dass bei Anordnung der Verkehrsdatenabfrage Name und Anschrift des Betroffenen sowie die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses anzugeben sind. Nur im Falle einer Straftat von erheblicher Bedeutung genügt gemäß § 100h I Satz 2 StPO eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn andernfalls die Erforschung des Sachverhalts aussichtslos oder wesentlich erschwert wäre. 18 Prozent der Befragten gaben an, dass sie diese Ausnahmeregelung gerne erweitert sähen. Dagegen soll die Regelung nach 75 Prozent der Befragten in ihrer jetzigen Fassung beibehalten werden. 7 Prozent der Befragten sprechen sich für eine Einschränkung aus.

Zur Begründung für eine Erweiterung der Regelung gaben sieben Befragte an, dass die Maßnahme nur mit einem geringfügigen Eingriff in die Grundrechte der Betroffenen verbunden sei. Die Eingriffsintensität sei niedrig. Weiter wurde angeführt (vier Befragte), dass auch die Aufklärung „einfacher“ Straftaten durch derartige Maßnahmen möglich sein sollte. Zudem wurde vorgeschlagen, dass die Anordnung auch bei zwar namentlich nicht bekannten, aber trotzdem individualisierbaren Betroffenen ermöglicht werden sollte. Teilweise seien gerade zu Beginn der Ermittlungen die genauen Personalien nicht bekannt. Es würden fingierte Daten bei der Beantragung des Anschlusses angegeben. Weiter wurde angegeben, dass Straftaten im Zusammenhang mit Telekommunikation und Internet zunehmen würden. Eine Erweiterung dieser Regelung würde nach Ansicht einiger Befragten zu einer effektiveren Strafverfolgung führen. Für die Beibehaltung der derzeitige Regelung führten die Befragten diverse Gründe an: 16 Befragte waren der Ansicht, dass die jetzige Regelung ausreichend sei. Je 15 Personen begründete ihre Antwort damit, dass sie bislang mit der jetzigen Fassung keine Probleme gehabt hätten und sich die Regelung bewährt habe. Weitere 13 Befragte finden die Vorschrift praktikabel. Sonstige Begründungen waren, dass so die Verhältnismäßigkeit gewahrt werde, dass die Regelung sachgerecht und ausgewogen sei und dass die Subsidiaritätsklausel eine Aufweichung des Bestimmtheitserfordernisses verhindere. Die Regelung entspreche dem

unterschiedlichen Gewicht der Delikte. Diejenigen Befragten, die sich für eine Einschränkung dieses Normabschnitts aussprachen, begründeten dies damit, dass die genauen Daten des Betroffenen oft nicht bekannt seien. Name und Anschrift seien häufig fingiert oder zunächst nicht ermittelbar, beispielsweise auch bei ausländischen, in Deutschland benutzten Anschlüssen. Telefone würden oft gewechselt. SIM-Karten würden auf einen beliebigen Namen angemeldet. Oftmals könne gerade erst durch die Maßnahme der Anschlussinhaber ermittelt werden. Die Anforderungen an die Bestimmtheit des Betroffenen sollen nach diesen Befragten also herabgesetzt werden, da – auch bei Straftaten, die nicht von erheblicher Bedeutung sind – nähere Informationen über den Täter ansonsten fehlen, die grundsätzlich aber verfügbar sind. Die Angaben darüber, inwieweit Straftaten, die nicht von erheblicher Bedeutung sind, wegen dieser Regelung nicht aufgeklärt werden können, schwanken von nie (9 Prozent) bis häufig (16 Prozent), wobei gelegentlich (46 Prozent) die meistgenannte Kategorie ist (selten 29 Prozent).

d) Sonstige Unklarheiten der jetzigen Regelungen

Die Frage, ob es aus ihrer Sicht Unklarheiten bzgl. der Regelungen der §§ 100g, 100h StPO gebe, verneinten 80 Prozent und bejahten 20 Prozent der Befragten. Letztere gaben folgende Unklarheiten an: Die Abgrenzung zwischen § 113 TKG und §§100g, 100h StPO bei dynamischen IP-Adressen sei problematisch (37 Prozent). Ebenfalls zu dieser Thematik gehört die als schwierig empfundene Abgrenzung zwischen Verkehrsdaten und Bestandsdaten (5 Prozent). 13 Prozent der Befragten finden den Begriff der Straftat von erheblicher Bedeutung unklar. Außerdem wurde angegeben, dass die Regelung allgemein unklar bzw. unverständlich (9 Prozent), zu „kompliziert“ (9 Prozent) und „unübersichtlich“ (4 Prozent) sei. Zudem sei fraglich, welche Daten genau erhoben werden dürfen, der Anwendungsbereich sei ungenau und es sei zu unbestimmt, was konkret unter den Begriff der „Verkehrsdaten“ falle (16 Prozent). Inwieweit die Verkehrsdatenabfrage einen noch unbekannten Täter erfasst, ist nach Ansicht von 5 Prozent ebenfalls nicht explizit geregelt. Als weitere Unklarheiten wurden das Auslesen von Mobiltelefondaten, der Begriff der Zielwahlsuche sowie die Frage, ob auch eine Straftat, die mittels Endeinrichtung begangen wurde, erheblich sein muss, angeführt.

2. Aktenanalyse

Die Problematik der Abgrenzung der Verkehrsdatenabfrage zur Personendatenabfrage nach § 113 TKG wurde auch im Rahmen der Aktenanalyse aufgegriffen. Ob bei der Auskunft über Verkehrsdaten zu IP-Adressen statische oder dynamische IP-Adressen zugrunde lagen, ließ sich den Akten nicht entnehmen. Es wurden nur die IP-Adressen an sich erwähnt oder aufgelistet. Nur in 14 Fällen wurden Daten zu IP-Adressen abgefragt. Diese Abfragen betrafen acht Verfahren. Die Vermutung liegt nahe, dass es sich größtenteils um dynamische IP-Adressen gehandelt haben muss, da überwiegend private Anschlüsse abgefragt wurden. Allerdings lässt sich dies bei ISDN- und DSL-Anschlüssen nicht bestätigen. Auch ob ein solcher Anschluss vorlag, konnte den Akten oftmals nicht entnommen werden. Daher lässt sich auch nicht genau sagen, aufgrund welcher Rechtsgrundlage Personendaten zu dynamischen IP-Adressen abgefragt wurden. Wie bereits erörtert wurde, ist die Rechtsgrundlage sowohl in der Rechtsprechung als auch in der Literatur umstritten. Aufgenommen werden konnte nur, ob eine Personendatenabfrage zu einer Rufnummer oder einer IP-Adresse aus einem Beschluss erfolgte und auf welche Rechtsgrundlage dieses Ersuchen gestützt wurde. Eine solche Abfrage erfolgte bei 12 Prozent der Anschlüsse (191). Dabei wurden unterschiedliche gesetzliche Grundlagen herangezogen. 22-mal wurde dabei auf §§ 100g, 100h StPO zurückgegriffen, wenn auch in manchen Fällen vorher nach § 113 TKG vorgegangen worden war. Das Auskunftsverlangen wurde in diesen Fällen allerdings vom jeweiligen Netzbetreiber abgelehnt und ein Beschluss nach §§ 100g, 100h StPO verlangt (bei acht Beschlüssen). Überwiegend wurde jedoch auf die Normen des TKG abgestellt (§ 89 VI, 90 TKG a.F. bzw. §§ 112, 113 TKG n. F. – bei 68 Anschlüssen). 23-mal wurde sowohl auf §§ 100g, 100h StPO als auch auf die Normen des TKG Bezug genommen. Sechsmal ließ sich den Akten entnehmen, dass eine „SARS-Abfrage“ erfolgte. Dabei handelt es sich um eine Online-Abfrage von Personendaten, die durch die Polizeibeamten selbst vorgenommen werden kann[457]. Zweimal wurde auf § 161a StPO zurückgegriffen. Im Übrigen konnte den Akten die Nennung einer Rechtsgrundlage nicht entnommen werden (bei ca. einem Drittel der Personendatenabfragen). Zu berücksichtigen ist außerdem, dass aus den Akten nicht ersichtlich war, ob die Richter teilweise – entgegen ihrer Überzeugung – Beschlüsse nach §§ 100g, 100h StPO in diesen Fällen erlassen haben, da sie wussten, dass die Anbieter die Herausgabe der Daten sonst verweigern würden und sie den Ermittlungserfolg nicht beeinträchtigen wollten.

3. Experteninterviews

a) Polizeibeamte

(1) Veränderungen gegenüber der Regelung in § 12 FAG

Die Schlüsselpersonen wurden ebenfalls zu Veränderungen der Praxis der Auskunftserteilung durch die Regelung der Verkehrsdatenabfrage in §§ 100g, 100h StPO gegenüber der Regelung in § 12 FAG befragt. Am häufigsten wurde darauf verwiesen, dass nunmehr auch zukünftige Daten erfasst seien. § 12 FAG habe nur Daten aus der Vergangenheit erfasst. Das sei eine Erleichterung der Arbeit. Die IMEI-Überwachung habe es früher nicht gegeben. Weiter wurde angegeben, dass der taktische Einsatzraum sich verändert habe. Früher sei das Ermittlungsverhalten eher tatorientiert gewesen, heute sei es täterorientiert. § 12 FAG habe zudem eher den Festnetzbereich betroffen, während §§ 100g, 100h StPO auch

[457] Dabei handelt es sich offensichtlich um die Abfrage nach § 112 TKG.

Mobilfunkbetreiber und Internetanbieter anspreche. Fünf der befragten Polizeibeamten haben keine spürbaren Veränderungen durch die Regelung der Verkehrsdatenabfrage in § 100g, 100h StPO im Vergleich zur Regelung in § 12 FAG wahrgenommen.

(2) Schwächen und Unklarheiten

Aus der Sicht von etwa der Hälfte der Befragten gibt es keine Unklarheiten und Schwächen der Regelungen der §§ 100g, 100h StPO. Es gebe keine Anwendungsprobleme und demnach bestehe auch kein Änderungsbedarf. Die Regelung sei einleuchtend. Weiter wurde angegeben, dass nicht klar geregelt sei, wie lange die Daten gespeichert werden sollen, in welchem Format und wann sie angeliefert werden müssten. Das könne man für die Praxis handhabbarer machen. Die Daten kämen oft sehr spät und es sei unklar, ob sie vollständig seien. Das nicht geregelte Antwort-Zeit-Verhalten mache sich in der Praxis bemerkbar. Es sollte gesetzlich festgelegt werden, wann und in welcher Form, nämlich elektronisch, geliefert werden müsse. Die elektronische Form sei notwendig, da bei einer Funkzellenabfrage ein Abgleich per Hand kaum möglich sei. Ein Befragter gibt an, dass die Lieferung innerhalb einer Woche wünschenswert sei. Es werde Zeit, dass die Vorratsdatenspeicherung eingeführt werde. Die Daten würden zu früh gelöscht. Manchmal werde eine Straftat erst nach einem Jahr bekannt.

Weiter wurde als Schwäche aufgeführt, dass die Telekommunikationsanbieter nicht verpflichtet würden, das Anonymisierungsverfahren für Behörden auszuschalten. Anonymisierte Daten würden nicht weiterhelfen. Weiter seien auch ausgeschaltete Mobiltelefone (im Standby-Betrieb) interessant für die Polizei. Mobiltelefone loggen sich auch im Standby-Betrieb in die Funkzellen ein. Diese Daten würden aber nicht mitgeliefert. Problematisch sei auch, dass Daten aus dem Ausland nicht erhoben werden könnten. Es handle sich oft um reisende Täter, die sich in den Niederlanden, der Türkei oder in Polen aufhielten. Ohne Rechtshilfeersuchen seien diese Daten nicht zu erlangen. Die Speicherfristen im Ausland seien unbekannt und dann ggf. bereits abgelaufen. Ein Rechtshilfeersuchen dauere zu lang. Beim sog. Phishing oder bei Kfz-Diebstählen ende die Verkehrsdatenabfrage an den nationalen Grenzen.

Eine Unklarheit wird auch für die Abgrenzung zwischen §§ 100gh StPO und § 113 TKG betont. Es sollte gesetzlich festgelegt werden, ob IP-Adressen als Verbindungs- oder Bestandsdaten zu behandeln seien. Die Regelung sollte eindeutig sein und keinen Interpretationsspielraum zulassen. Es gebe dabei immer wieder Probleme. Ein anderes Problem beziehe sich auf den Nachweis der tatsächlichen Kommunikation bei einer Funkzellenabfrage.

b) Staatsanwälte

(1) Veränderungen gegenüber der Regelung in § 12 FAG

Die Hälfte der befragten Staatsanwälte hat seit der Einführung von §§ 100g, 100h StPO keine Veränderungen der Verkehrsdatenabfrage gegenüber § 12 FAG für die Praxis wahrgenommen. Fünf Befragte führten an, dass früher nur rückwirkende Daten erfasst waren, heute könne man auch zukünftige Daten abfragen. Dass nun auch zukünftige Daten erfasst seien, stelle eine Erleichterung dar. Aber die Bedeutung sei relativ gering, denn wenn eine Telefonüberwachung möglich sei, werde diese durchgeführt und liefere die Verkehrsdaten mit. Nur wenn keine Katalogtat, sondern eine andere Straftat von erheblicher Bedeutung vorliege, spiele die Verkehrsdatenabfrage eine Rolle. Die Voraussetzungen seien etwas angehoben worden (Subsidiarität, erhebliche Bedeutung). Vorher habe man auch bei einfacheren Delikten die Maßnahme durchführen können. Aufgrund des Begriffs der „Straftat von erheblicher Bedeutung“ sei die Maßnahme in bestimmten Bereichen nicht mehr möglich. Zudem sei durch die Verpflichtung zur Löschung ein erhöhter Arbeitsaufwand entstanden. Vorher sei es keine Standardmaßnahme gewesen. Bei § 12 FAG habe es Streit darüber gegeben, ob Standortdaten erfasst waren. Das sei jetzt klar definiert.

(2) Schwächen und Unklarheiten

Eine Schwäche der Regelungen der §§ 100g, 100h StPO sei, dass Name und Anschrift des Anschlussinhabers angegeben werden müssten. Es sei aber selten, dass der Anschlussinhaber auch der Nutzer ist. Es sei problematisch, diesen zu ermitteln. Gerade bei Computerdelikten handle es sich in der Regel um unbekannte Täter. Die Anforderung des § 100h I Satz 1 StPO, Name und Anschrift anzugeben, sei nicht zu erfüllen. Hier sei eine Klarstellung erforderlich (obwohl die gerichtliche Praxis den Beschluss einfach erlasse).

Schwierigkeiten würde auch die Abgrenzung zwischen TKG und §§ 100g, 100h StPO verursachen. Es gebe in diesem Zusammenhang hauptsächlich Probleme mit dynamischen IP-Adressen. Hier wäre, so die Interviewten, eine Klarstellung gut.

Eine zumindest vorläufige Speicherung bzw. Sicherung der Daten sei wünschenswert. Ein sehr großes Thema seien ferner Auslandsstraftaten. In diesem Feld seien Veränderungen unerlässlich. Gerade beim sog. Phishing, würden die Server im Ausland stehen. Rechtshilfeersuchen würden wegen zu kurzer Speicherfristen ins Leere laufen. Die Daten würden in der Zwischenzeit verloren gehen. Es sei sinnvoll, eine europäische Zentralstelle einzurichten, denn die Computerkriminalität sei grenzüberschreitend und international. Ein Befragter ist der Ansicht, dass die §§ 100 ff. StPO insgesamt übersichtlicher gestaltet werden sollten. Die Eingriffsmaßnahmen seien unstrukturiert. Begriffe wie „aussichtslos oder wesentlich erschwert“ würden hier und da ins Gesetz gestreut. Bei § 100a StPO gebe es einen Katalog, bei § 100g StPO knüpfe man daran an, aber es gebe wiederum auch andere Möglichkeiten. Beim verdeckten Ermittler gebe es einen ganz leichten Katalog, beim Lauschangriff einen starken. Ein Befragter erwähnt, dass eine Spezialisierung der Behörden bei allen verdeckten Ermittlungsmaßnahmen sinnvoll wäre. Hierfür sollte es eine gemeinsame Abteilung geben. Die Hälfte der Befragten meinen, dass es keine Schwächen oder Unklarheiten der Regelung gebe.

c) Richter

(1) Veränderungen gegenüber der Regelung in § 12 FAG

Auch bei den befragten Richtern hat die Hälfte keine Veränderungen der Praxis wahrgenommen, seit sie in §§ 100g, 100h StPO geregelt ist und nicht mehr in § 12 FAG. Rechtlich seien nicht viele Veränderungen bewirkt worden, führt einer der Befragten aus, entscheidende Veränderungen seien aber durch die tatsächliche Lage entstanden. Es habe früher nicht so viele Mobiltelefone und technische Möglichkeiten gegeben. Deshalb sei auf die Nutzung von Verkehrsdaten relativ selten zurückgegriffen worden. §§ 100g, 100h StPO seien zudem klarer formuliert. Früher seien die zukünftigen Daten nicht erfasst und die Löschung der Daten sei ein Problem gewesen.

(2) Schwächen und Unklarheiten

Schwächen und Unklarheiten sehen etwa die Hälfte der Befragten nicht. Es bestehe kein Regelungsbedarf. Die Normen seien ausreichend, dürfen aber auch nicht weitergehend sein. Ein Befragter findet die Regelungen sehr kompliziert. Aber das sei eine allgemeine Erscheinung bei den §§ 100a ff. StPO. Es wäre besser, wenn die Regelungen transparenter und strukturierter wären, so dass sich der Inhalt besser erschließen würde. Unklar formuliert seien die Vorschriften, was die Eilanordnung betreffe. Immer wieder stelle sich die Frage, ob die Eilanordnung innerhalb von drei Tagen bestätigt werden müsse oder nicht. Eine weitere Schwäche sei die Abgrenzung zwischen §§ 100g, 100h StPO und § 113 TKG. Es gebe immer wieder Auseinandersetzungen mit den Anbietern, was die Benennung der Anschlussinhaber angeht.

Ein Befragter ist der Ansicht, es fehle eine Regelung für vermisste Kinder. §§ 100g, 100h StPO solle nur zur Aufklärung von Straftaten dienen. Aber wenn ein Kind oder eine ältere, verwirrte Person vermisst werde und ein Mobiltelefon in der Tasche habe, wäre es sinnvoll, die Maßnahme auch dann zuzulassen. Dann könne man feststellen, wo sich das Kind befinde. Das sei aber zur Zeit nicht möglich. Man könne nicht davon ausgehen, dass eine Straftat vorliege. Man müsse konstruieren, dass das Kind entführt worden sei, wofür aber meist gar kein Anhaltspunkt bestehe. Ein Befragter gab an, dass auch bei den Prepaid-Karten die Daten gespeichert werden sollten. Dass diese Daten momentan nicht gespeichert würden, öffne straftatenbezogener Nutzung mobiler Kommunikation „Tür und Tor“. §§ 100g, 100h StPO würden zu wenig zwischen den einzelnen Anwendungsfällen unterscheiden. Bei der Erstellung eines Bewegungsbildes sei der Richtervorbehalt wichtig, bei anderen Anwendungsbereichen nicht.

d) Verteidiger

(1) Veränderungen gegenüber der Regelung in § 12 FAG

Als Änderungen durch die Regelung in §§ 100g, 100h StPO gegenüber der Regelung der Verkehrsdatenabfrage in § 12 FAG wurde von Verteidigerseite zum einen angegeben, dass die Hürde der Eingriffsvoraussetzungen (Straftat von erheblicher Bedeutung, Katalogtat) höher gesetzt worden sei. Zudem werde die Ermittlungsmaßnahme nunmehr erst von der Staatsanwaltschaft überprüft. Außerdem habe der Mobilfunkverkehr zugenommen und das Kommunikationsverhalten habe sich insgesamt verändert. Dadurch sei auch die Zahl der Verkehrsdatenabfragen gestiegen.

(2) Schwächen und Unklarheiten

Unklarheiten und Schwächen betreffen aus Sicht der Verteidiger, dass die Normen zu abstrakt und zu offen seien. Es sei für Strafverfolgungsbehörden zu einfach, die Maßnahmen durchzusetzen. Außerdem sei der Begriff „erheblich“ äußerst dehnbar. Problematisch sei auch die Frage, ob die mittels Endeinrichtung begangenen Straftaten ebenfalls erheblich sein müssen. Zumindest der Bagatellbereich sollte ausgeschlossen werden. Zudem sei der Wortlaut hinsichtlich der Voraussetzung, dass Name und Anschrift angegeben werden müssen, unklar. Es werde die Meinung vertreten, dass auch Ermittlungen gegen Unbekannt zulässig seien. Die Normen würden vom Wortlaut her nicht zum Internetbereich passen, so dass eine gesonderte Norm vorzugswürdig sei. Weiter wird bemängelt, dass große Unsicherheiten bezogen auf die Abgrenzung des § 113 TKG zu den §§ 100g, 100h StPO bestünden. Letztendlich könnte die Staatsanwaltschaft aber zu den schärferen Normen greifen, da diese ohnehin genehmigt würden. Präzisierungsbedarf bestünde auch bezüglich der Datenspeicherung. Die Netzbetreiber dürften nur zu Auskünften über solche Informationen verpflichtet werden, die sie legalerweise besitzen dürfen. In dieser Hinsicht sei der Wortlaut uneindeutig und eine verfassungskonforme Auslegung notwendig.

Zum anderen sei die Normanwendung problematisch. Es sei unklar, welcher Verdachtsgrad vorliegen müsse, um die Maßnahme anzuordnen. Schwierigkeiten bereite auch die Frage, ob der Sachverhalt für die Anordnung der Maßnahme ausreichend gewesen sei oder wegen Unverhältnismäßigkeit nicht hätte angeordnet werden dürfen, da noch andere, weniger in die Rechte des Betroffenen eingreifende Maßnahmen in Betracht kamen. Problematisch sei auch die Handhabung der Zeugnisverweigerungsrechte, wenn z. B. das Angehörigenverhältnis unklar war.

e) Telekommunikationsunternehmen

(1) Unklarheiten und Schwächen

Unklarheiten und Schwächen der Vorschriften §§ 100g, 100h StPO wurden von fast allen Befragten gesehen. Diese betreffen zuvorderst die von den Providern reklamierte Prüfungskompetenz. Zum einen sollte klargestellt werden, dass auf eine Eilanordnung hin eine richterliche Bestätigung erfolgen müsse. Zum anderen sei es wünschenswert, wenn die Netzbetreiber die Verhältnismäßigkeit beanstanden könnten. Der Richtervorbehalt erfülle seine Funktion nicht mehr, eine ernsthafte Prüfung finde kaum noch statt. Die Betroffenen sollten zudem benach-

richtigt werden. In Bezug auf die zukünftigen Verkehrsdaten sei unklar, in welchen Intervallen die Auskünfte erteilt werden sollen, meint ein Mobilfunkbetreiber. Die tägliche Datenlieferung sei ihnen aus technischen Gründen nicht möglich. Die Festnetzbetreiber seien dazu übergegangen, für die zukünftigen Verkehrsdaten ihre Überwachungssysteme zu nutzen. Sie würden die Daten über diese Systeme direkt an die Bedarfsträger weiterleiten. Im Festnetzbereich würden die §§ 100g, 100h StPO demnach wie bei Überwachungsmaßnahmen gehandhabt – quasi online würden die Verkehrsdaten an die Bedarfsträger übermittelt. Es sei unklar, wer Nachrichtenmittler sei und ob darunter auch das Opfer falle. Hier fände keine willentliche Kontaktaufnahme statt. Konturenlosigkeit entstünde dadurch, dass alle (auch unwillentliche) Kontaktaufnahmen durch den Täter erfasst werden. Eine weitere Unklarheit sei die Formulierung „räumlich und zeitlich hinreichend bestimmte Telekommunikation“ in § 100h StPO.

(2) Verbesserung der Abwicklung der Verkehrsdatenabfrage

Von den befragten Telekommunikationsunternehmen halten alle Befragten die Abwicklung der Auskunftserteilungen für verbesserungswürdig. Dabei wurden verschiedene Aspekte angesprochen. Ein einheitliches Verfahren sei sinnvoll, d. h. einheitliche Anfragen und Beschlüsse. Wenn die Anforderung von einer zentralen Stelle übermittelt würde, würde dies die Bearbeitung erleichtern. Zudem sei eine Spezialisierung von einzelnen Staatsanwaltschaften und Gerichten wünschenswert. Eine zentrale Zuständigkeit eines Gerichtes für alle Anordnungen wird vorgeschlagen bzw. eine Zentralstelle pro Bundesland und pro Bundesbehörde. Es sei wichtig, mit informierten Stellen zu sprechen. Allein die Technik und die juristische Bewertung seien kompliziert. Geschultes Personal würde die Arbeit erleichtern. Dadurch würde die Qualität der Anordnungen zunehmen und die Quantität abnehmen. Weiter wurde ein flächendeckendes automatisiertes Verfahren als wünschenswert angesehen. Die Arbeitszeiten würden reduziert und Ressourcen gespart. Dadurch sei auch das Vorantreiben der Ermittlungen möglich. Ebenso sei dies bei der Rechnungsstellung sinnvoll. Im Moment müssten die Anbieter für jede Maßnahme eine Rechnung erstellen.

Auch an der Lesbarkeit und Klarheit der Beschlüsse müsse noch gearbeitet werden. Es sei überlegenswert, Standardformulare zu entwerfen. Derzeit sei jeder Beschluss anders. Eine klare Begrenzung von Beschlüssen in örtlicher und zeitlicher Hinsicht sei ebenfalls wünschenswert. Explizit angesprochen wurde auch, dass die Entschädigung reibungslos verlaufen sollte. Manche Behörden würden nicht freiwillig zahlen (Mahnung) oder Einzelabrechnungen monieren. Das treibe die Kosten zusätzlich in die Höhe.

(3) Vorratsdatenspeicherung

Alle befragten Vertreter der Telekommunikations-Unternehmen haben sich gegen die Vorratsdatenspeicherung ausgesprochen. Das Bundesverfassungsgericht habe die Vorratsdatenspeicherung klar als unzulässig angesehen. Der Speicherzweck stehe in diesem Fall noch nicht fest. Zudem entstünde ein permanenter Überwachungsdruck. Es handle sich um einen nachhaltigen Eingriff in die Privatsphäre der Kunden und um eine anlasslose Sammlung der Daten aller Bürger. Ein Befragter ist der Ansicht, dass wir „auf dem Weg zum Orwell-Staat“ seien und nicht weit entfernt vom „gläsernen Bürger“. Der ursprüngliche Anlass für die Vorratsdatenspeicherung seien Straftaten wie Terrorismus, organisierte Kriminalität und Kinderpornographie gewesen. Nun solle die Abfrage der Daten aber bei jeder Straftat mittels Endeinrichtung angeordnet werden, meint einer der Befragten. Andere verweisen darauf, dass neue, noch zu entwickelnde Systeme erforderlich würden. Dies bringe eine erhebliche Belastung für die Unternehmen mit sich und sei mit hohen Kosten verbunden. Die Vorratsdatenspeicherung würde zu einem deutlichen Anstieg von Anordnungen führen. Heute seien die Daten oftmals bereits gelöscht gewesen. Die Speicherung an sich koste nicht viel, erklärt ein Befragter, aber die effiziente Durchsuchung der riesigen Datenmengen (in angemessener Zeit) werde schwierig. Das sei nur mit hocheffizienter Hard- und Software möglich. Der Vorschlag, dass der Staat die Maßnahmen selbst durchführt, sei abgelehnt worden. Dies beruhe darauf, dass die Kosten ausschlaggebend gewesen seien.

Weiter wurde ausgeführt, dass die Vorratsdatenspeicherung nicht effektiv zur Aufklärung zu nutzen sei. Die Polizei sei mit der Datenmenge überfordert. Bisher sei die Speicherung Kundenentscheidung gewesen und 60 Prozent der Kunden hätten die Löschung Ihrer Daten beantragt. Dass bedeute für die Anbieter, dass 60 Prozent mehr Daten gespeichert werden müssen. Die Vorratsdatenspeicherung bedeute für das Unternehmen eines des Befragten voraussichtlich einen zusätzlichen Investitionsaufwand von 8 Millionen Euro zu Beginn und weiteren zwei Millionen Euro pro Jahr. Ein weiterer Befragter erklärt, dass die Vorratsdatenspeicherung (beim Zielwahlsuchlauf) das 60-fache Datenvolumen mit sich bringen würde. Die Vorratsdatenspeicherung werde wegen anonymisierender Proxys im Ergebnis aber nichts bringen. IP-Adressen würden dabei ausgetauscht bzw. simuliert. Diese Anonymisierungsproxys seien allgemein verbreitet, auch außerhalb der EU. Dadurch würden die Abfragen ins Leere gehen bzw. Personen zu Unrecht beschuldigt werden. Auch im Festnetzbereich gebe es Manipulationsmöglichkeiten (andere Nummer erscheint). Zudem würde die gleiche IMEI-Nummer sehr oft vergeben und könne manipuliert werden. Das gleiche treffe für die Rechneridentifizierung (MAC-Adresse) zu. Sinnvoller wäre nach Ansicht von einem Befragten das „Quick-freeze“-Verfahren. Die Unternehmen gaben an, dass über die Verbände versucht worden sei, die Vorratsdatenspeicherung zu verhindern bzw. zu begrenzen. Man hätte versucht, dies auf einen bestimmten Rahmen zu reduzieren. Man habe verhindern wollen, dass noch zusätzliche Daten erfasst werden sollten, die bisher nicht erfasst würden. Die Verbände seien auch bemüht gewesen, die Speicherungsdauer zu reduzieren.

f) Datenschützer

(1) Schwächen und Unklarheiten

Als Schwäche der Regelungen wurde von den Datenschutzbeauftragten der weite Anwendungsbereich der Normen genannt. Es müssten eben keine erheblichen Straftaten vorliegen.

(2) Verbesserungsvorschläge für die zukünftige Gestaltung

Als Verbesserungsvorschlag für die zukünftige Abwicklung der Auskunftserteilungen wurde u. a. eine effektive Kontrolle von Anträgen angeführt, insbesondere dahingehend, dass auch entlastende Aspekte berücksichtigt werden sollen. Auch die Vorbereitung der Anordnung sollte sorgfältiger erfolgen. Der Richter sollte die Ermittlungsakte bekommen und sich bei Fragen an die Staatsanwaltschaft wenden können. Weiter wurde angeführt, dass eine Statistik sinnvoll sei, um die Entwicklung der Maßnahmen zu beobachten und um festzustellen, welche Delikte den Anordnungen zugrunde lagen. Dadurch würde auch eine rechtsstaatliche Kontrolle dieser Anordnungen gewährleistet. Zudem sei die Benachrichtigung problematisch. Eine zukünftige Prüfung, ob tatsächlich benachrichtigt wird, wäre sinnvoll. Ein anderer Vorschlag betraf einen möglichst eng ausgestalteten Straftatenkatalog.

(3) Vorratsdatenspeicherung

Die Vorratsdatenspeicherung wird von allen befragten Datenschützern kritisch bzw. negativ beurteilt. Von einem Befragten wurde sie als „datenschutzrechtlicher Sündenfall“ bezeichnet. Die Vorratsdatenspeicherung verstoße gegen sämtliche datenschutzrechtliche Grundkonzepte. Teilweise meinten die Befragten, dass diese Datensammlung auf Vorrat verfassungswidrig sei. Sie hoffen, dass die Richtlinie vor dem EuGH geprüft werde. Es werde mehr gespeichert als notwendig sei. Das sei auch für die Provider eine Zumutung. Die Datenflut sei kaum beherrschbar. Aufwand und Kosten seien immens, da eine unglaublich große Menge an Daten gesammelt werden sollen. Die Datenermittlungen würden grenzenlos, das Internet ermittelbar gemacht. Das sei maßlos und laufe rechtsstaatlichen Prinzipien entgegen. Die Anbieter seien zu „Handlangern“ der Strafverfolgungsbehörden geworden. Es sei auch fraglich, ob die Daten für die Strafverfolgung überhaupt effektiv nutzbar seien.

Weiter wurde die Hoffnung geäußert, dass die nationale Regelung weicher ausfalle als die EU-Richtlinie. Es bleibe abzuwarten, ob die Klage Irlands die Richtlinie aufgrund ihrer fragwürdigen Rechtsgrundlage noch werde aufhalten können. Die Datenschutzbeauftragten hätten eine Stellungnahme abgegeben, aber auf Landesebene seien die Einflussmöglichkeiten relativ gering. Die anlass- und verdachtslose Speicherung für den Fall, dass die Daten irgendwann gebraucht werden könnten, sei bisher verboten gewesen.

Angeführt wurde zudem, dass die Vorratsdatenspeicherung nunmehr nicht mehr für den ursprünglichen gedachten Zweck, nämlich Terrorismus und organisierte Kriminalität, verwendet werden würde, sondern auch für andere Straftaten und ggf. noch für weitere Zwecke. Nun sei auf einmal auch von Urheberrechtsverletzungen die Rede. Die Vorratsdatenspeicherung sei nach Ansicht eines Datenschutzbeauftragten vor allem deshalb riskant, da sie Muster für Speicherungen auf Vorrat auch in anderen Bereichen sein könne. Es könnte ein zentraler Datenpool entstehen, die Zwecke könnten immer weiter ausgedehnt würden. Die Technik schaffe die Versuchung, sie auch zu nutzen. Als Alternative wäre das „Quick-Freeze-Verfahren“ vorstellbar gewesen, wobei die Daten, die für die Rechnungsstellung gespeichert wurden, und dann auch zukünftige Daten aus einem ganz konkreten Anlass erhoben und gespeichert werden würden.

Wenn die Vorratsdatenspeicherung eingeführt werde, müssten auch die Eingriffsvoraussetzungen verschärft werden. Bagatellen sollten nicht darunter fallen. Der Straftatenkatalog des § 100a StPO sei zudem sehr weit. Die Hürden sollten höher gesetzt werden und der Subsidiaritätsgrundsatz strenger beachtet werden. Der Richtervorbehalt sei weiterhin wichtig, obwohl er – wie verschiedene Studien zeigten – kein allzu großes Hindernis darstelle. Die Benachrichtigung solle häufiger stattfinden. Zudem sollten die Kosten nach Ansicht eines Befragten nicht von den Anbietern getragen werden müssen.

4. Zusammenfassung der Ergebnisse

Befragung und Interviews führten zur Identifizierung verschiedener Probleme bei der Anwendung der §§ 100g, 100h StPO. Alle Untersuchungsmodule gaben Hinweise darauf, dass die Abfrage von Personendaten zu dynamischen IP-Adressen uneinheitlich gehandhabt wird. Während die befragten Netzbetreiber teilweise der Ansicht sind, dass es eines Beschlusses nach §§ 100g, 100h StPO bedürfe, sind die meisten befragten Polizeibeamten, Staatsanwälte und Richter der Meinung, dass § 113 TKG einschlägig sei und es keines Beschlusses bedürfe. Teilweise wird von den Staatsanwälten und Richtern angegeben, dass sie entgegen ihrer Überzeugung Beschlüsse nach §§ 100g, 100h StPO erließen, um die Ermittlungen nicht zu behindern, da sie wüssten, dass die Netzbetreiber sich weigern würden. Zudem richteten sich die Beteiligten nach unterschiedlichen Gerichtsurteilen. Von den meisten Befragten angesprochener ungeklärter Diskussionspunkt ist die Frage, ob nach einer Eilanordnung eine richterliche Bestätigung erfolgen müsse, damit die Daten herausgegeben werden. Die Netzbetreiber fordern teilweise einen Beschluss zur Herausgabe der Daten. Bis zur Bestätigung würden die Daten zunächst nur gespeichert. Die Justizbehörden sind dagegen teilweise der Ansicht, dass es keines richterlichen Bestätigungsbeschlusses bedürfe.

Als Problem wird offensichtlich auch gesehen, dass Name und Anschrift des Anschlussinhabers angegeben werden müssen. Häufig ist die Ausgangslage von Ermittlungen aber dadurch bestimmt, dass ein Anschlussinhaber erst ermittelt werden muss. Weiter wurde von Polizeibeamten angegeben, dass die fehlende gesetzliche Regelung

zur Speicherdauer sowie zur Form der Übersendung problematisch sei. Dass die Daten aus dem Ausland nicht erhoben werden könnten, würde zudem die Ermittlungen behindern. Ferner wird von den Befragten das Problem genannt, dass die Regelungen kompliziert und unverständlich seien. Die Normanwendung bereite Schwierigkeiten. Die Netzbetreiber befürworten ein vereinheitlichtes und standardisiertes Verfahren. Sie hielten es für sinnvoll, dass die Ansprechpartner auf Seiten der Strafverfolgungsbehörden konzentriert werden und geschultes Personal, ggf. in einer zentral zuständigen Behörde, eingesetzt werde. Zudem wird auf mangelnde Klarheit und Verständlichkeit der Beschlüsse hingewiesen.

Zur Vorratsdatenspeicherung wurden die Telekommunikationsanbieter sowie die Datenschützer befragt. Beide Gruppen halten die Vorratsdatenspeicherung für rechtlich bedenklich, teilweise sogar für verfassungswidrig. Die anlasslose Speicherung der Daten aller Bürger sei mit dem Grundgesetz nicht vereinbar und löse das Gefühl eines „permanenten Überwachungsdrucks“ bei den Bürgern aus. Teilweise wird davon gesprochen, dass Deutschland auf dem Weg zum Überwachungsstaat sei. Zudem seien die Massen der Daten kaum effektiv auszuwerten und der Aufwand für die Netzbetreiber sowie die Kosten, die wiederum von ihnen übernommen werden sollen, immens. Stattdessen befürworten die Befragten das sog. Quick-Freeze-Verfahren, bei dem die Daten, falls ein Verdacht vorliegt, gespeichert werden könnten bis ein Beschluss erlassen wird. Zudem wird kritisiert, dass nunmehr statt von Terrorismus und Bekämpfung von Kinderpornographie von Urheberrechtsverletzungen, wegen denen die auf Vorrat gespeicherten Daten herausgegeben werden könnten, die Rede sei. Das sei nicht verhältnismäßig.

D. Verhältnis der Verkehrsdatenabfrage zu anderen Ermittlungsmaßnahmen

Gegenstand der Evaluation ist auch das Verhältnis der Verkehrsdatenabfrage zu anderen Ermittlungsmaßnahmen. Dabei wurde vor allem das zeitliche Verhältnis der Maßnahmen, aber auch die Bedeutung der Verkehrsdatenabfrage im Vergleich zu anderen Ermittlungsmaßnahmen, insbesondere zur Telefonüberwachung, für das Ermittlungsverfahren untersucht.

I. Schriftliche Befragung

1. Verhältnis zur Telekommunikationsüberwachung

a) Kombinierte Anwendung der Verkehrsdatenabfrage mit der Telekommunikationsüberwachung

Bei der Beantwortung der Frage nach der Häufigkeit der kombinierten Anwendung von Verkehrsdatenabfrage und Telekommunikationsüberwachung zeigten sich bei der schriftlichen Befragung starke Unterschiede je nach Dezernatszugehörigkeit (siehe Tabelle 22).

So gaben auf der einen Seite Staatsanwälte aus den Dezernaten Betäubungsmittel, organisierte Kriminalität und Kapitaldelikte an, dass die Maßnahmen nach §§ 100g, 100h StPO im Jahr 2005 häufig mit Telekommunikationsüberwachungsmaßnahmen kombiniert wurden. Auf der anderen Seite stehen die Ergebnisse der Befragten aus Allgemeindezernaten sowie Dezernaten, die Jugend-, Verkehrs- und Internetstrafsachen bearbeiten. Hier gaben die Befragten zu 47 Prozent an, diese Maßnahmen nie zu kombinieren. Dies dürfte daran liegen, dass bei den entsprechenden Deliktstypen sehr selten eine Telekommunikationsüberwachung zur Anwendung kommt. Gerade bei Internetstrafsachen wird eine Telekommunikationsüberwachung praktisch nicht vorkommen. Bei den Dezernaten, die sich mit Wirtschafts-, Sexual- und sonstigen Straftaten befassen, zeigt sich im Antwortverhalten eine Polarisierung. Einerseits wird zu 30 Prozent angegeben, dass die Maßnahmen nie kombiniert werden. Auf der anderen Seite werden zu 52 Prozent die Kategorien „gelegentlich“ und „häufig“ genannt.

Tabelle 22

Kombination von Auskunftsersuchen mit Telekommunikationsüberwachungsmaßnahmen

Dezernatstypen	nie	selten	gelegentlich	häufig	immer	Anteil Antworten
Betäubungsmittel, organisierte Kriminalität und Kapitaldelikte	*2,7 %*	*9,0 %*	*25,2 %*	*55,0 %*	*8,1 %*	*99 %*
Wirtschaft, Sexualdelikte, sonstige	*30,3 %*	*13,7 %*	*24,4 %*	*27,3 %*	*4,3 %*	*84 %*
Allgemein, Jugend, Verkehr, Internet	*46,6 %*	*20,6 %*	*20,6 %*	*8,8 %*	*3,4 %*	*82 %*
Insgesamt	***31,9 %***	***15,4 %***	***23,2 %***	***24,9 %***	***4,6 %***	***85 %***

b) Zeitliches Verhältnis

Zu gleichen Teilen (jeweils zu ca. 46 Prozent) wurde von den Befragten angegeben, dass die Verkehrsdatenabfrage früher oder zeitgleich zur Telekommunikationsüberwachung durchgeführt werde. Nur 6 Prozent der Befragten gaben an, dass die Verkehrsdatenabfrage später erfolgte. Dies ist erwartungsgemäß, denn offensichtlich wird die Verkehrsdatenabfrage in die Telekommunikationsüberwachung integriert. Die Befunde aus der MPI Studie zur Überwachung der Telekommunikation haben ergeben, dass die mittelbaren Erfolge (insbesondere bei der Verfolgung von Betäubungsmitteldelikten) ganz im Vordergrund stehen[458]. Dies beruht ganz wesentlich darauf, dass durch die Überwachung der Kommunikationsinhalte Gesprächsteilnehmer festgestellt werden, die als Tatverdächtige in Betracht kommen.

c) Erfolgsaussichten der kombinierten Anwendung

Die Erfolgsaussichten der kombinierten Anwendung von Verkehrsdatenabfrage und Telekommunikationsüberwachung wurden im Allgemeinen hoch eingeschätzt. So gaben 15 Prozent der Befragten, die diese Frage beantwortet haben (618 Befragte bzw. 70 Prozent), an, dass diese sehr hoch seien, weitere 58 Prozent beurteilten die Erfolgsaussichten mit hoch, 23 Prozent mit mittelmäßig und nur 5 Prozent schätzten sie als (sehr) niedrig ein.

d) Kriminalistisches Verhältnis zwischen Verkehrsdatenabfrage und Telekommunikationsüberwachung

Bezüglich des Verhältnisses von Verkehrsdatenabfrage und Telekommunikationsüberwachung wurden 15 Fragen gestellt, die von 76 Prozent der Befragten beantwortet wurden. 24 Prozent der Befragten ließen diesen Fragenkatalog komplett aus. Welches Verhältnis nach den Angaben der Befragten zwischen Telefonüberwachung und Verkehrsdatenabfrage besteht, wird in Tabelle 23 detailliert dargestellt.

Dabei fällt auf, dass die beiden Fragen danach, welche der beiden Maßnahmen zu stichhaltigeren Beweisen führen, Inkonsistenzen aufweisen. So beantworteten z. B. 344 Befragte beide Fragen mit Nein (sieben mit jeweils Ja). Gleiches gilt für die Frage, welche der Maßnahmen erfolgversprechender ist. Hier antworteten 393 der Befragten zu beiden Varianten mit Nein und sechs Befragte jeweils mit Ja. Das kann so interpretiert werden, dass beide Maßnahmen hinsichtlich des erwarteten Erfolgs sowie der Stichhaltigkeit der hieraus resultierenden Beweise als vergleichbar eingeschätzt werden.

[458] *Albrecht/Dorsch/Krüpe*, 2003, S. 374ff.

Tabelle 23

Ermittlungspraktisches Verhältnis Verkehrsdatenabfrage zur Telekommunikationsüberwachung

Fragestellungen	Anteil ja (in %)
Verkehrsdatenabfrage ist kostengünstiger	*51,7*
Verkehrsdatenabfrage ist erfolgversprechender	*8,6*
Verkehrsdatenabfrage ist schneller	*42,3*
Verkehrsdatenabfrage ist einfacher auszuwerten	*41,5*
Verkehrsdatenabfrage führt zu stichhaltigeren Beweisen	*5,3*
Verkehrsdatenabfrage wird öfter bewilligt als TKÜ	*18,9*
Verkehrsdatenabfrage ist in best. Fallkonst. sinnvoller als TKÜ	*18,5*
Verkehrsdatenabfrage ist bei best. Delikten sinnvoller als TKÜ	*5,7*
TKÜ erfordert mehr Arbeitsaufwand	*59,4*
TKÜ ist eingriffsintensiver	*66,9*
TKÜ führt zu stichhaltigeren Beweisen	*44,1*
TKÜ betrifft weniger Personen	*8,3*
TKÜ ist erfolgversprechender	*33,2*
TKÜ ist in best. Fallkonst. sinnvoller als Verkehrsdatenabfrage	*25,1*
TKÜ ist bei best. Delikten sinnvoller als Verkehrsdatenabfrage	*14,9*

Auf die Frage, ob die Verkehrsdatenabfrage in bestimmten Fallkonstellationen sinnvoller als die Telekommunikationsüberwachung ist, antworteten 18,5 Prozent mit Ja. Ein Drittel der Befragten, die diese Frage mit Ja beantwortet haben, führte dies freitextlich weiter aus. Am häufigsten wurde dabei genannt, dass die Verkehrsdatenabfrage dann sinnvoll sei, wenn es um Daten aus der Vergangenheit, um retrograde Daten, gehe (43 Prozent). Außerdem sei der Nachweis der Kontakte oft ausreichend und genau diese Kontakte seien mit der Abfrage der Verkehrsdaten festzustellen (16 Prozent). Zudem sei die Abfrage der Daten dann sinnvoller als die Telekommunikationsüberwachung, wenn es darum geht, den Täter zu ermitteln (14 Prozent). Zu 9 Prozent gaben die Befragten an, dass die Verkehrsdatenabfrage immer dann sinnvoller sei, wenn es nicht auf den Inhalt der Gespräche ankomme. Weitere 9 Prozent sind der Ansicht, dass die Auskunft über die Daten der Vorbereitung der Telekommunikationsüberwachung diene und 4 Prozent gaben an, dass anhand der Verkehrsdaten oftmals entschieden werden könne, ob eine Telekommunikationsüberwachung notwendig sei. 9 Prozent meinen, dass die Verkehrsdatenabfrage zur Feststellung von Standortdaten, zur Erstellung eines Bewegungsprofils und zum Nachweis der Anwesenheit am Tatort bedeutender sei. Schließlich wurde noch angegeben, dass die Abfrage der Verkehrsdaten in solchen Fällen bedeutend sei, in denen keine Katalogtat nach § 100a StPO vorliege (4 Prozent). Insoweit käme der Verkehrsdatenabfrage auch eine Auffangfunktion zu.

Auf die Frage, ob die Verkehrsdatenabfrage bei Vorliegen bestimmter Delikte sinnvoller als die Telekommunikationsüberwachung ist, antworteten 5,7 Prozent der Befragten mit ja. Explizit wurden von jeweils fünf Befragten mittels Endeinrichtung begangene Delikte oder Fälle, in denen keine Katalogtat i. S. d. § 100a StPO gegeben sei, aufgeführt. Zwei weitere Befragte gaben den Betrug an. Die Telekommunikationsüberwachung soll dagegen nach Ansicht von 25 Prozent der Befragten in bestimmten Fallkonstellationen sinnvoller sein als die Verkehrsdatenabfrage. 15 Prozent der Befragten hielten sie bei bestimmten Delikten für sinnvoller. 155 der Befragten (18 Prozent) gaben bei den Fragen nach bestimmten Fallkonstellationen bzw. Delikten noch eine freitextliche Antwort, die in ihren wesentlichen Punkten in Tabelle 24 zusammengefasst sind.

Die genannten Delikte zeichnen sich dadurch aus, dass bei Ihnen eine Tatbegehung durch eine Gruppe von Tätern Voraussetzung oder wahrscheinlich ist. Damit soll die Telekommunikationsüberwachung helfen, die konkre-

Tabelle 24

Delikte und Fallkonstellationen, bei denen die Telekommunikationsüberwachung sinnvoller erscheint

Delikte bzw. Fallkonstellationen	Nennungen	Prozent der Nennungen	Häufigkeit der Nennungen
Betäubungsmitteldelikte	38	*23 %*	*28 %*
Bandenmäßige Betäubungsmitteldelikte	5	*3 %*	*4 %*
Bandendelikte	10	*6 %*	*8 %*
Organisierte Kriminalität	9	*5 %*	*7 %*
Schleusungen	8	*5 %*	*6 %*
Erpressungen	4	*2 %*	*3 %*
Immer, wenn es auf Gesprächsinhalte ankommt	59	*35 %*	*44 %*
Ermittlungen in die Zukunft	4	*2 %*	*3 %*
VD reichen nicht, sagen nichts aus	9	*5 %*	*7 %*
VD nicht ausreichend, um Nutzer zu identifizieren	4	*2 %*	*3 %*
Klärung der Bandenstrukturen	3	*2 %*	*2 %*
Absprachen	6	*4 %*	*5 %*
Identifizierung von Tatbeteiligten	4	*2 %*	*3 %*
Wenn Straftat noch andauert	4	*2 %*	*3 %*
Feststellung von Kontakten	2	*1 %*	*2 %*
	169	***100 %***	***126 %***

ten Bandenstrukturen sowie Absprachen zwischen den Gruppenmitgliedern festzustellen. Von den Delikten wurden insbesondere Betäubungsmitteldelikte und Bandendelikte sowie deren Kombination genannt. In Einzelfällen wurde in diesem Zusammenhang angegeben, dass die Kombination aus §§ 100g, 100h StPO und § 100a StPO sinnvoll sei, insbesondere auch in dem Sinne, dass die Verkehrsdatenabfrage für die Vergangenheit und die Telekommunikationsüberwachung für die Zukunft angewandt werde. Auf die Frage, ob es rechtliche oder praktische Verbesserungsmöglichkeiten bei der kombinierten Anwendung einer Maßnahme nach §§ 100g, 100h StPO und einer Telekommunikationsüberwachung gebe, antworteten 65 Prozent mit nein, 5 Prozent mit ja und 30 Prozent enthielten sich. Neun Befragte gaben an, dass eine Erweiterung der Katalogtaten des § 100a StPO wünschenswert sei, wobei vor allem die Erweiterung auf alle banden- und gewerbsmäßigen Delikte gefordert wurde. Weitere Änderungsvorschläge (jeweils von drei Befragten) waren die längere Datenspeicherung und die Abschaffung bzw. Einschränkung des Richtervorbehalts.

2. Verhältnis zu anderen Ermittlungsmaßnahmen

a) Kombinierte Anwendung der Verkehrsdatenabfrage mit anderen Maßnahmen

Auf die Frage, inwieweit andere Ermittlungsmaßnahmen mit der Verkehrsdatenabfrage kombiniert werden[459], gaben die Befragten mehrheitlich an, dass Beschlagnahme und Durchsuchung gelegentlich bis häufig neben der Abfrage der Daten angeordnet würden (Tabelle 25). Etwas seltener waren die Observation und der Einsatz technischer Mittel in Kombination mit §§ 100g, 100h (selten bis gelegentlich). Als nächstes folgen der Einsatz verdeckter Ermittler und die Postbeschlagnahme (nie bis selten). Schließlich wurden noch – wenn auch sehr selten – die (Raster)Fahndung und die Wohnraumüberwachung erwähnt. Damit zeigt sich, dass nach Einschätzung der Befragten die Verkehrsdatenabfrage auch häufig mit offenen Ermittlungsmaßnahmen kombiniert wird.

Sonstige von den Befragten angegebenen, mit §§ 100g, 100h StPO kombinierten Maßnahmen, sind Telekommunikationsüberwachung (58 Prozent der Nennungen unter sonstiges, wobei dies im nächsten Abschnitt des Fragebogens behandelt wurde), Bankauskunft (14 Prozent), Vernehmungen und V-Personen (jeweils 9 Prozent) und § 100i StPO (8 Prozent).

b) Zeitliches Verhältnis

In Bezug auf die zeitliche Reihenfolge gaben 66 Prozent an, dass die Verkehrsdatenabfrage vor anderen Maßnahmen durchgeführt werde. Weitere 19 Prozent nannten eine zeitgleiche Ausführung der Maßnahmen. 7 Prozent berichteten, dass die Verkehrsdatenabfrage nach den anderen Maßnahmen vollzogen werde. 8 Prozent gaben Kombinationen an, wobei teilweise auch auf die Einzelfallabhängigkeit hingewiesen wurde[460].

c) Typische Fallkonstellationen

Auf die Frage, welche typischen Fallkonstellationen es bei kombinierter Anwendung von Verkehrsdatenabfrage mit anderen Ermittlungsmethoden gibt, nannten

[459] Ca. 30 Prozent der Befragten beantworteten diese Frage nicht, wobei sie entweder die Frage insgesamt unbeantwortet ließen (14 Prozent der Befragten) oder auch nur einzelne Maßnahmen ausließen.

[460] Unbeantwortet ließen die Frage 20 Prozent der Befragten. Sie wurden bei der Prozentuierung nicht berücksichtigt.

Tabelle 25

Verhältnis zu anderen Ermittlungsmaßnahmen (Angaben in Prozent)

	nie	selten	gelegentlich	häufig	immer	keine Antwort
Beschlagnahme	*8,5*	*11,2*	*25,4*	*31,4*	*3,3*	*20,3*
Postbeschlagnahme	*38,7*	*23,3*	*6,3*	*1,4*	*0,1*	*30,2*
(Raster-)Fahndung	*44,6*	*14,8*	*5,5*	*3,3*	*0,5*	*31,4*
Wohnraumüberwachung	*46,9*	*12,1*	*5,0*	*3,5*	*0,8*	*31,6*
Einsatz technischer Mittel	*24,4*	*17,6*	*16,9*	*9,6*	*1,4*	*29,9*
Durchsuchung	*5,6*	*7,7*	*21,3*	*41,9*	*5,1*	*18,4*
Einsatz verdeckter Ermittler	*31,6*	*22,3*	*12,2*	*4,0*	*0,6*	*29,3*
Observation	*22,7*	*17,8*	*18,9*	*12,8*	*1,3*	*26,5*
Sonstige	*4,6*	*1,6*	*1,3*	*2,4*	*1,1*	*89,0*

70 Prozent der Befragten sowohl eine Beschlagnahme des Telefons, Rechners und von Datenträgern zur Ermittlung von Verkehrsdaten sowie eine Durchsuchung, um diese Gegenstände zu finden und Verkehrsdaten zu ermitteln. Die Häufigkeit wurde im Mittel mit gelegentlich eingestuft, wobei Beschlagnahme als etwas häufiger eingeschätzt wurde. Zu erwähnen sind speziell von den Befragten frei formulierte Kombinationen. So wurde in 3 Prozent der Fälle angegeben, dass eine typische Fallgestaltung darin zu sehen sei, dass durch Verkehrsdaten der Verdächtige identifiziert werde und anschließend eine Durchsuchung bei diesem stattfinde. Ebenso häufig wurde eine Kombination der Verkehrsdatenabfrage mit der Telekommunikationsüberwachung oder mit einer Durchsuchung nach sonstigen Beweismitteln genannt.

II. Aktenanalyse

Aus der Auswertung der Verfahrensakten ergibt sich vor allem das zeitliche Verhältnis der Verkehrsdatenabfrage zu anderen Ermittlungsmaßnahmen.

1. Zeitpunkt der Anordnung der Verkehrsdatenabfrage im Ermittlungsverfahren

Wie in Abbildung 99 dargestellt, dauerte die Ermittlungsphase der ausgewerteten Verfahren bis zu über 36 Monate (das längste Verfahren dauerte fünf Jahre). Am häufigsten war eine Dauer von drei bis vier Monaten und vier bis fünf Monaten.

Über diese allgemeine Betrachtung hinaus, wurde untersucht, zu welchem Zeitpunkt im Ermittlungsverfahren die erste Maßnahme nach §§ 100g, 100h StPO angeordnet wurde.

Die Dauer der Verfahren bis zur Anordnung der Verkehrsdatenabfrage wird aus Abbildung 100 ersichtlich. Ein beachtlicher Teil der Abfrage entfällt bereits auf die ersten Tage nach Einleitung eines Ermittlungsverfahrens. In knapp 40 Prozent der Verfahren erfolgt die Anordnung einer Abfrage innerhalb der ersten Woche. Mehr als vier Fünftel der Anträge sind nach zwei Monaten gestellt. In 5,4 Prozent der Verfahren wurde die Verkehrsdatenabfrage erst nach sechs Monaten angeordnet.

In 64 Prozent der Verfahren war die Verkehrsdatenabfrage der Grund für die erste Einschaltung der Staatsanwaltschaft[461]. Allgemeine Anzeigen gingen in 11 Prozent und Anregungen von Telekommunikationsüberwachungsmaßnahmen in 10 Prozent der Verfahren voraus. Dieses Ergebnis macht deutlich, dass die Verkehrsdatenabfrage, wenn sie Bestandteil der Ermittlungen ist, zumeist eine der ersten Maßnahmen im Ermittlungsverfahren darstellt.

[461] Mehrfachnennungen waren möglich.

Abbildung 99



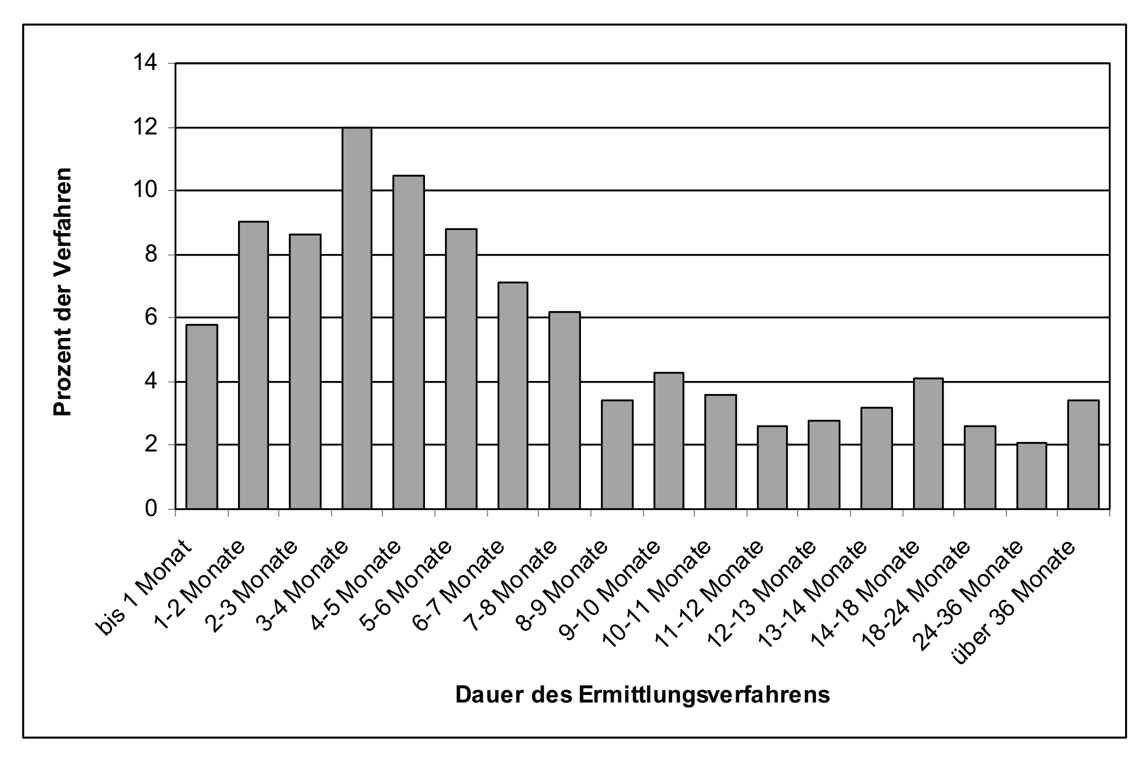
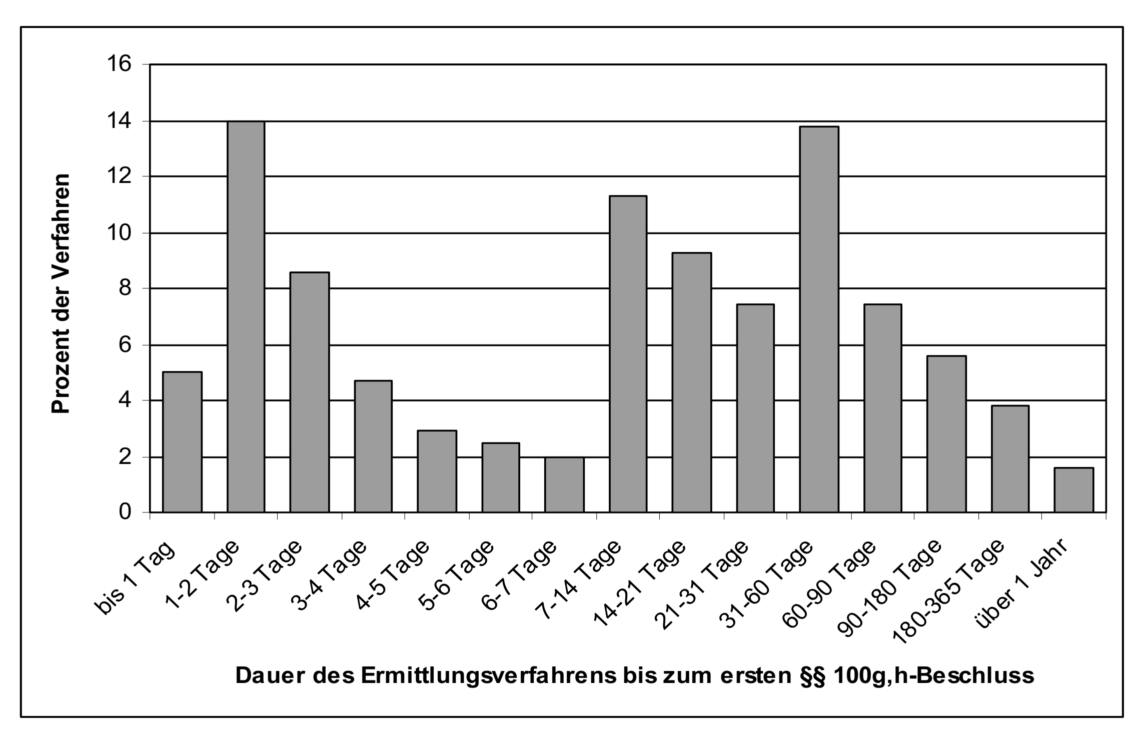


Abbildung 100



Dauer des Ermittlungsverfahrens bis zum ersten Beschluss nach §§ 100g, 100h StPO



2. Sonstige Maßnahmen im Ermittlungsverfahren

Neben der Verkehrsdatenabfrage wurden in den untersuchten Verfahren zahlreiche andere Ermittlungsmaßnahmen durchgeführt. Wie häufig diese angeordnet wurden, ergibt sich aus Abbildung 101. In 70 Prozent der Verfahren wurden Zeugenvernehmungen durchgeführt und in 40 Prozent der Verfahren Durchsuchungen angeordnet. In 25 Prozent der Verfahren wurden Anschlussinhaberfeststellungen nach §§ 112, 113 TKG neben der Verkehrsdatenabfrage eingeleitet und in 24 Prozent der Verfahren Telekommunikationsüberwachungsmaßnahmen. Sonstige Maßnahmen, die ebenfalls recht häufig dokumentiert sind, betreffen u. a. Sicherstellungen und daktyloskopische Spurenuntersuchungen.

In 31 Verfahren wurden neben den Verkehrsdatenabfragen keine anderen Ermittlungsmaßnahmen durchgeführt. Welche Delikte diesen Verfahren zugrunde lagen, lässt sich Abbildung 102 entnehmen. Dabei ist zu berücksichtigen, dass mehrere dieser Delikte in einem Verfahren vorkommen konnten. Dies ist aber nur bei zwei Verfahren und jeweils zwei Delikten der Fall.

Am häufigsten wurden allein Maßnahmen nach §§ 100g, 100h StPO bei Verfolgung von Betrugsdelikten durchgeführt. Fast alle diese Betrugsdelikte wurden mittels Endeinrichtung begangen. In sieben Verfahren handelte es sich dabei um den „Enkeltrick“, in dem der Anrufer sich als Verwandter des meist schon älteren Opfers ausgibt und um Geld betrügt oder dies versucht. Häufig lediglich auf Verkehrsdatenabfragen beschränkt waren auch Ermittlungsverfahren wegen besonders schweren Fällen des Diebstahls. In fünf von sechs Fällen handelte es sich dabei um Einbrüche in Kraftfahrzeuge, bei denen das darin befindliche Mobiltelefon entwendet wurde. Ähnlich verhält es sich bei den Raubdelikten. Hier ging es in der Regel um Straßenraub, bei denen dem Opfer u. a. das Mobiltelefon abgenommen wurde. Im Übrigen wurden die meisten Delikte, die den Ermittlungsverfahren ohne andere Maßnahmen zugrunde lagen, mittels Endeinrichtung begangen (Bedrohung, Beleidigung, Androhung von Straftaten, räuberische Erpressung).

Abbildung 101

Ermittlungsmaßnahmen in den untersuchten Verfahren neben Verkehrsdatenabfrage

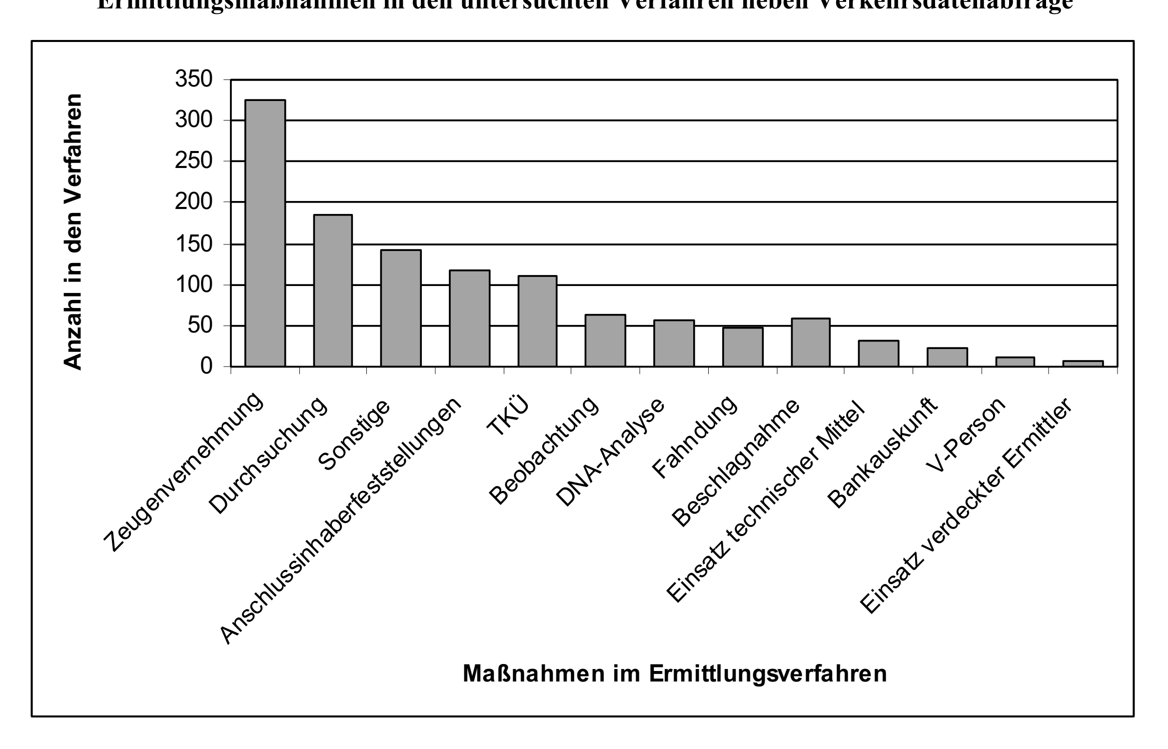
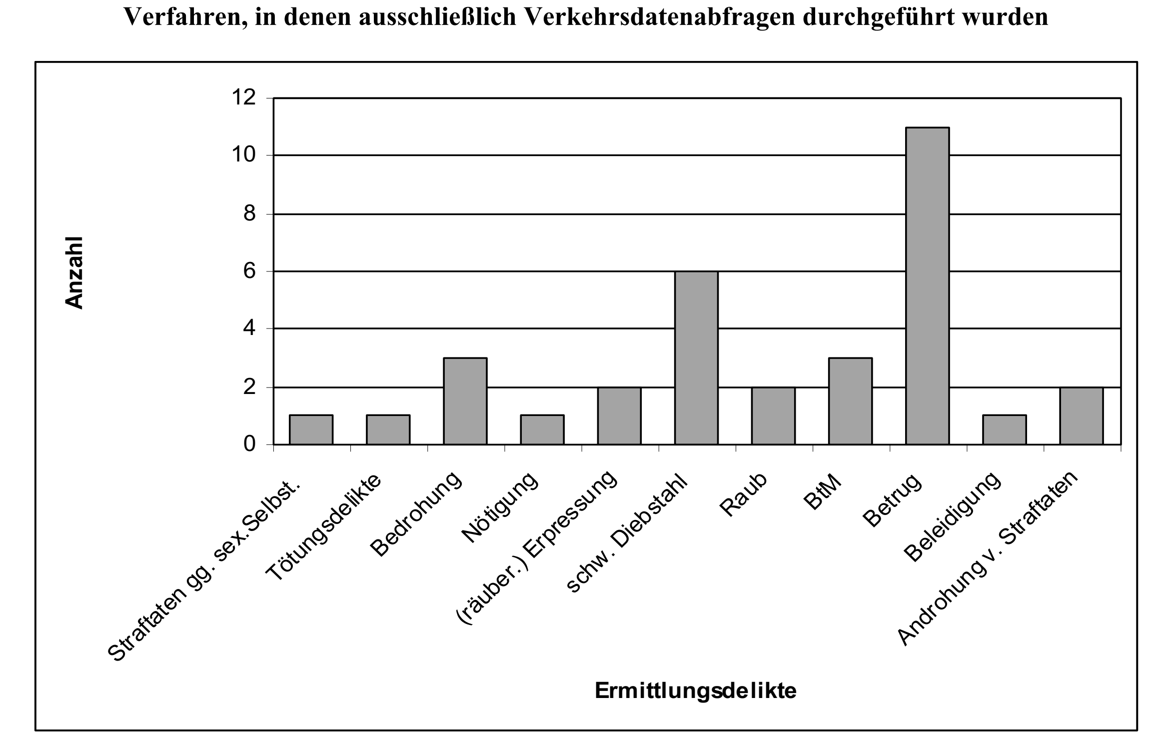


Abbildung 102

Verfahren, in denen ausschließlich Verkehrsdatenabfragen durchgeführt wurden



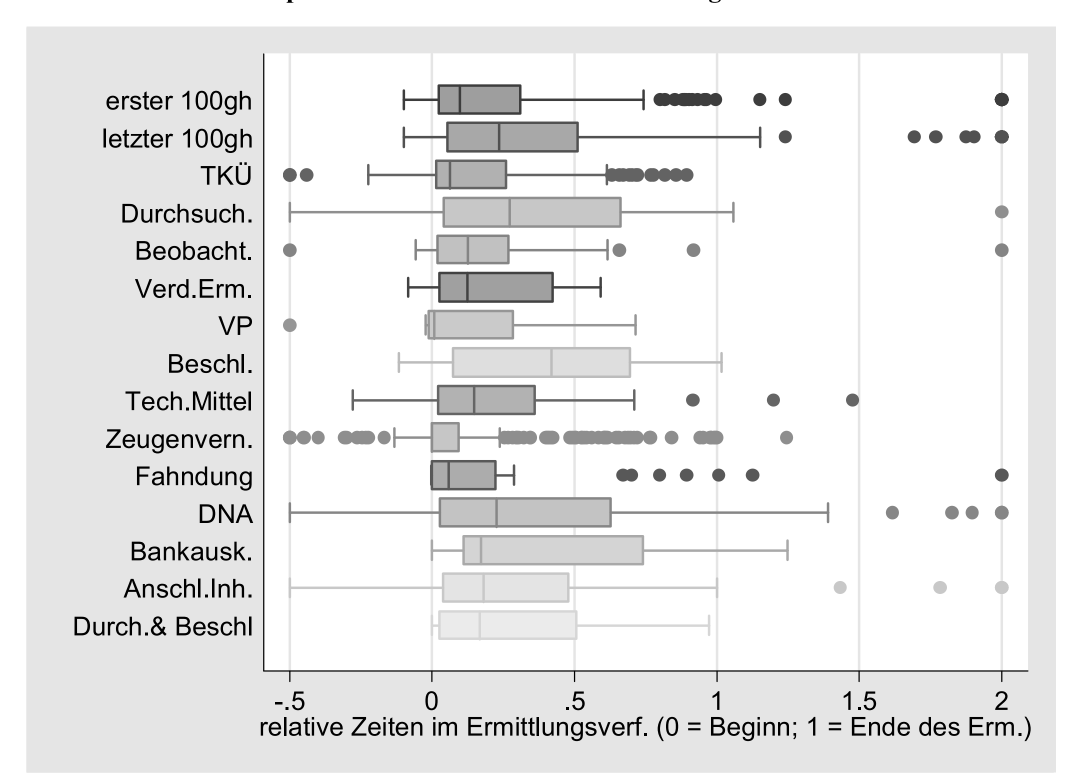
3. Zeitpunkt der Anordnung der Maßnahmen im Ermittlungsverfahren

Zu welchem Zeitpunkt des Ermittlungsverfahrens die Verkehrsdatenabfrage und im Vergleich dazu die anderen Maßnahmen angeordnet und durchgeführt wurden, lässt sich Abbildung 103 entnehmen. Wie bereits ausgeführt wurde, kennzeichnet 0 den Beginn des Ermittlungsverfahrens und 1 das Ende des Ermittlungsverfahrens. Der Strich in der Mitte der Boxen kennzeichnet den Median. Bei den Punkten vor und hinter den Boxen handelt es sich um Ausreißer. Bei den Punkten vor Beginn des Ermittlungsverfahrens handelt es sich fast immer um Maßnahmen aus anderen Verfahren, die mit dem ausgewerteten Verfahren verbunden wurden.

Der erste Beschluss nach §§ 100g, 100h StPO wird sehr früh im Ermittlungsverfahren erlassen. Früher setzen gelegentlich Telekommunikationsüberwachungsmaßnahmen ein, soweit diese überhaupt in dem Verfahren Anwendung finden. Der letzte Beschluss nach §§ 100g, 100h StPO erfolgte in der ersten Hälfte des Ermittlungsverfahrens. Durchsuchung und Beschlagnahme erfolgten über die Mitte des Ermittlungsverfahrens hinweg. Wenn sie zusammen angeordnet wurden, ist der Medianwert bei einem früheren Zeitpunkt angesiedelt, etwa bis zur Mitte des Ermittlungsverfahrens. Vertrauenspersonen scheinen schon von Beginn des Verfahrens an tätig zu sein. Dies wird darauf beruhen, dass durch ihre Hinweise erst das Ermittlungsverfahren ausgelöst wird. Ansonsten fällt auf, dass die Observation, der Einsatz verdeckter Ermittler, der Einsatz von technischen Mitteln, die Fahndung und die Anschlussinhaberfeststellungen innerhalb der ersten Hälfte des Ermittlungsverfahrens eingesetzt werden. Die Zeugenvernehmungen streuen sich über das gesamte Ermittlungsverfahren.

Abbildung 103

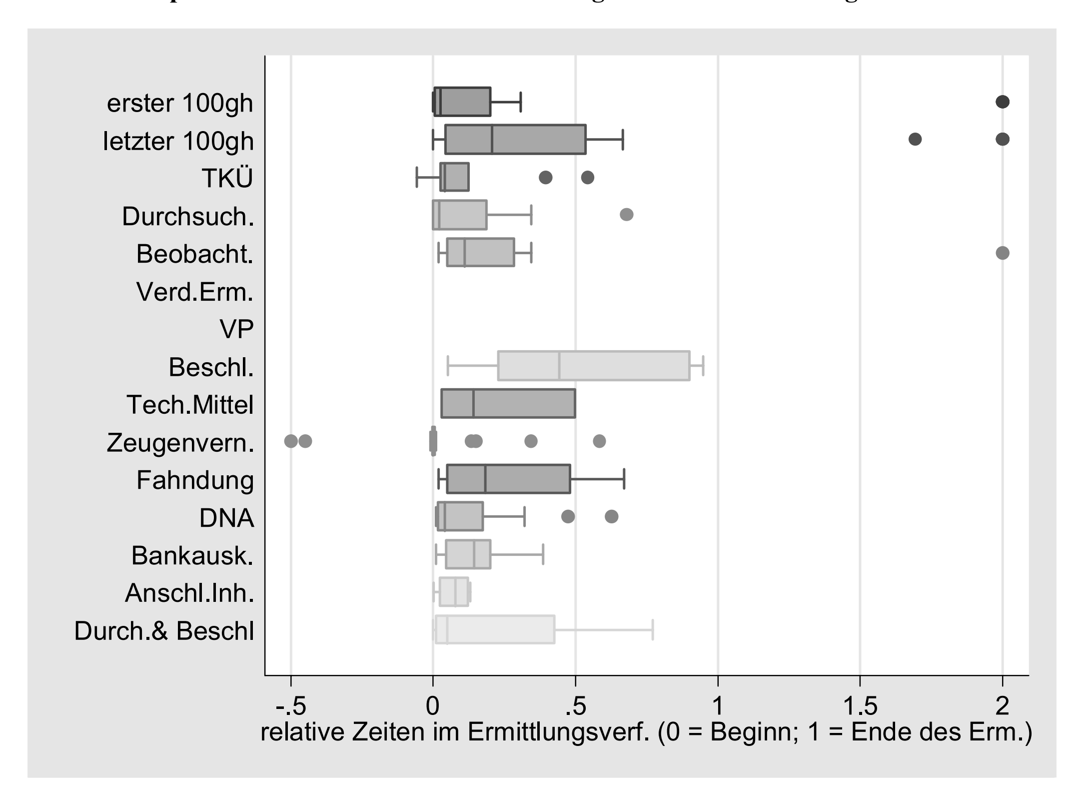
Zeitpunkt der Maßnahmen im Ermittlungsverfahren



Dabei sind Unterschiede hinsichtlich der den Verfahren zugrunde liegenden Delikte festzustellen. In Abbildung 104 wird dargestellt, wie sich der Einsatz der Maßnahmen im Ermittlungsverfahren bei Tötungsdelikten gestaltet. Abgesehen von der Beschlagnahme und dem letzten Beschluss nach §§ 100g, 100h StPO werden hier alle Maßnahmen innerhalb der ersten Hälfte des Ermittlungsverfahrens eingesetzt. Das wird wohl darauf beruhen, dass die Aufklärung von Tötungsdelikten mit Priorität behandelt wird.

Abbildung 104

Zeitpunkt der Maßnahmen im Ermittlungsverfahren bei Tötungsdelikten



Der erste Beschluss nach §§ 100g, 100h StPO erfolgt noch früher als bei der Gesamtbetrachtung. Der Median liegt unmittelbar am Anfang des Ermittlungsverfahrens. Der Einsatz der Telekommunikationsüberwachung liegt hier leicht hinter dem ersten Beschluss nach §§ 100g, 100h StPO. Das wird darauf zurückzuführen sein, dass erst anhand der Verkehrsdaten festgestellt werden soll, wer mit dem Getöteten Kontakt hatte und dann Telekommunikationsüberwachungsmaßnahmen geschaltet werden.

Bei Raubdelikten sowie (räuberischer) Erpressung verändert sich das Bild wie in Abbildung 105 gezeigt. Die Anordnung der Telekommunikationsüberwachung liegt hier etwas vor der Anordnung der Verkehrsdatenabfrage. Der erste Beschluss nach §§ 100g, 100h StPO wird wiederum innerhalb der ersten Hälfte des Ermittlungsverfahrens erlassen.

Bei Betäubungsmitteldelikten ist der erste Einsatz von Verkehrsdatenabfragen und Telekommunikationsüberwachungsmaßnahmen nahezu zeitgleich ausgestaltet. Das spricht dafür, dass die Maßnahmen zusammen angeordnet wurden, um die Strukturen der Geschäftsbeziehungen und Verbindungen festzustellen. Auffällig ist, dass die Fahndung sich hier fast über das gesamte Ermittlungsverfahren erstreckt. Die DNA-Analyse geht weit über den Zeitraum des Ermittlungsverfahrens hinaus. Dies könnte an molekulargenetischen Untersuchungen nach dem Zeitpunkt des polizeilichen Abschlußberichts, die durch die Staatsanwaltschaft veranlasst werden, liegen.

Bei den Betrugsdelikten liegen sowohl der Zeitpunkt des ersten als auch des letzten Beschlusses nach §§ 100g, 100h StPO beim Beginn des Ermittlungsverfahrens (Abbildung 107).

Neben Verkehrsdatenabfragen, Telekommunikationsüberwachungsmaßnahmen und Durchsuchungen spielen Bankauskünfte eine Rolle. Dabei kann es sich zum einen um Betrug zum Nachteil von Banken handeln, zum anderen können Auskünfte über die Konten des Beschuldigten und das ggf. darauf verbuchte, durch den Betrug erlangte Geld eingeholt werden. Dass die DNA-Analyse erst zum Ende des Ermittlungsverfahrens hin eingesetzt wird, spricht dafür, dass die Staatsanwaltschaft nach Abschluss des polizeilichen Handelns weitere Beweise sichern wollte.

Abbildung 105



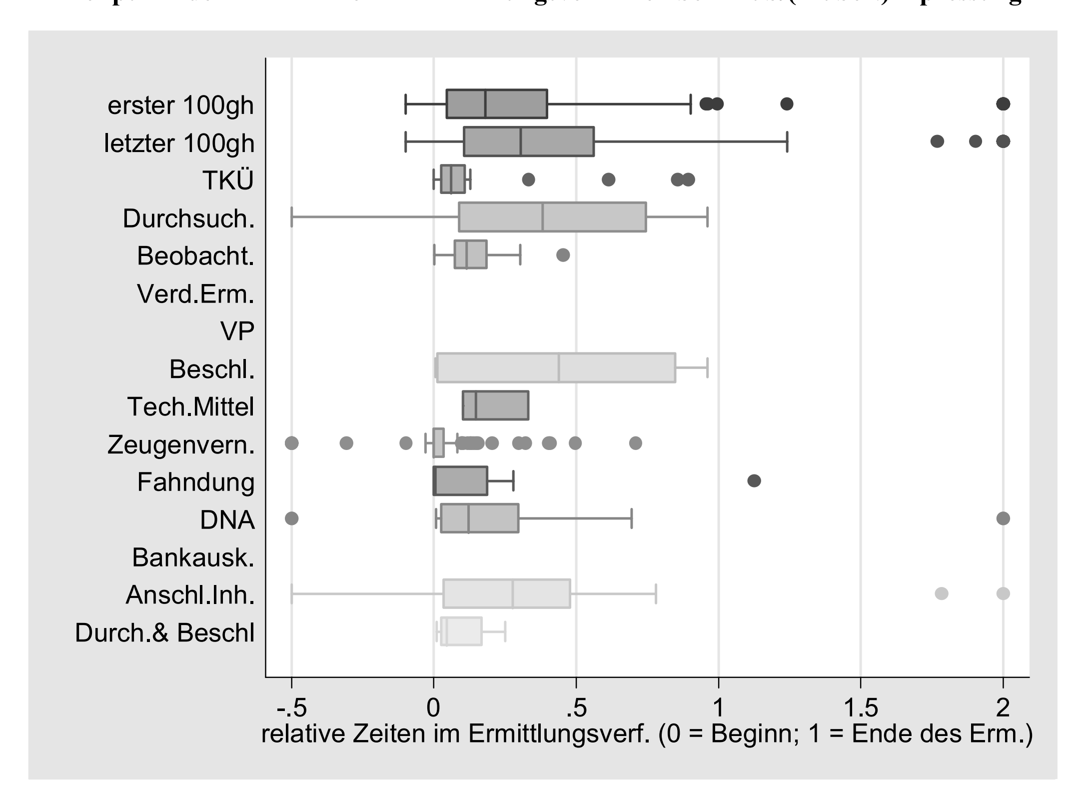


Abbildung 106

Zeitpunkt der Maßnahmen im Ermittlungsverfahren bei Betäubungsmitteldelikten

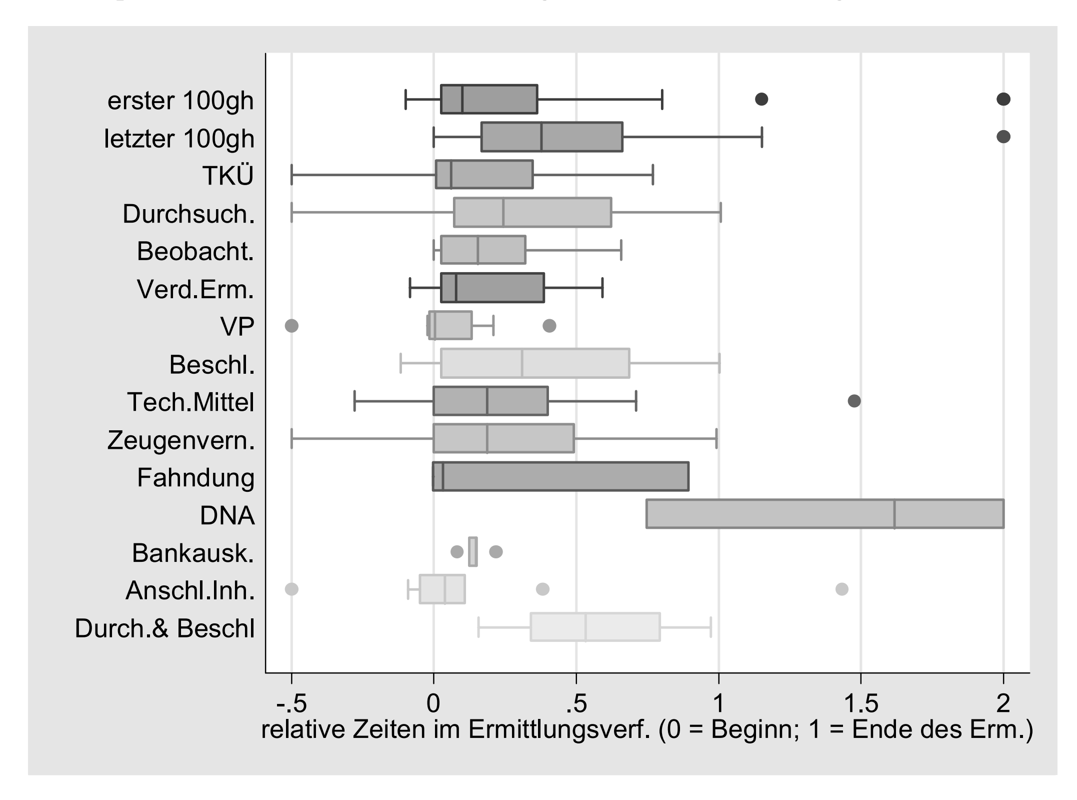
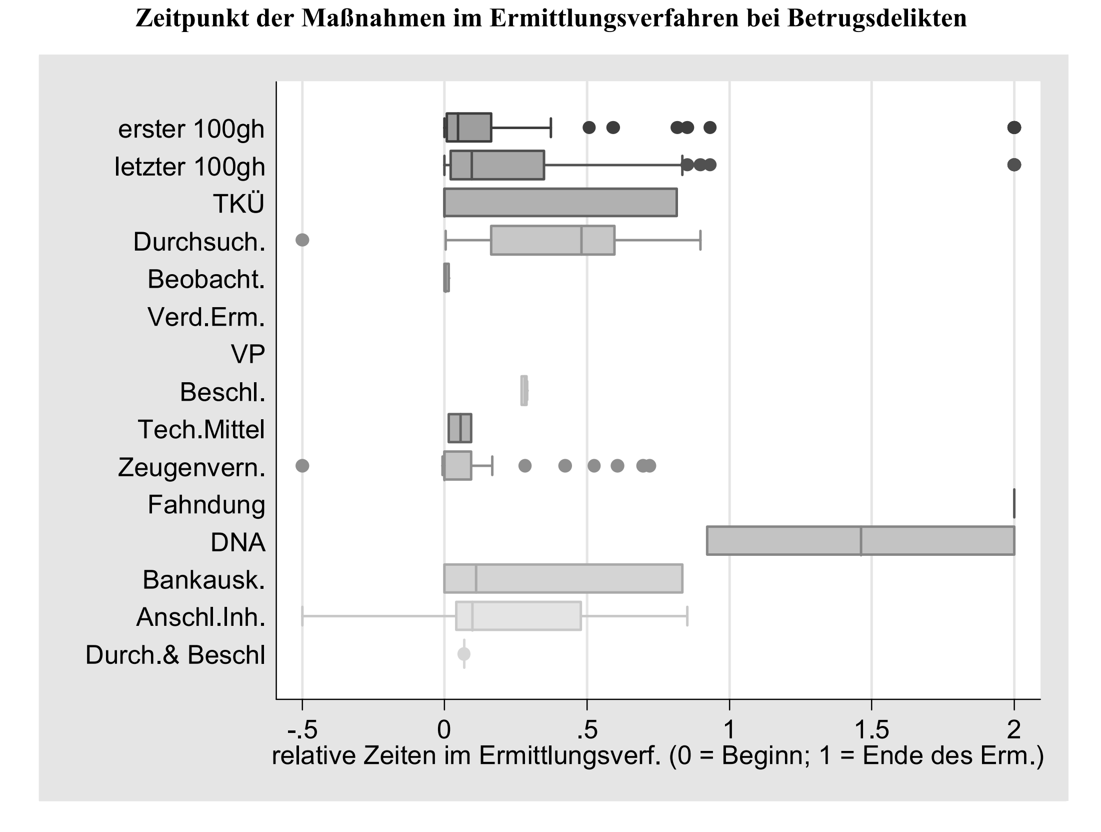


Abbildung 107

Zeitpunkt der Maßnahmen im Ermittlungsverfahren bei Betrugsdelikten



4. Dauer der Maßnahmen

Abbildung 108 beschreibt die Dauer der in den untersuchten Verfahren durchgeführten Maßnahmen. Dabei fällt auf, dass die Abfrage der Verkehrsdaten schwerpunktmäßig innerhalb der ersten 100 Tage des Ermittlungsverfahrens erfolgt bzw. die Dauer der Abfrage in diesen Zeitraum fällt. Die Telekommunikationsüberwachung ist im Vergleich dazu wesentlich kürzer und setzt erst später ein.

Abbildung 109 zeigt die Dauer der eingesetzten Maßnahmen differenziert nach Delikten. Dabei fällt auf, dass die Dauer der Verkehrsdatenabfrage bei Betrugsdelikten sehr kurz ist, während die Abfrage bei Betäubungsmitteldelikten und Tötungsdelikten über einen längeren Zeitraum erfolgt. Gerade bei den Betäubungsmitteldelikten war dies zu erwarten, da bei diesen das Geschehen erst über einen längeren Zeitraum beobachtet und Beweise gesammelt werden, bevor die Verdächtigen angeklagt werden.

Abbildung 108

Dauer der Maßnahmen in Tagen

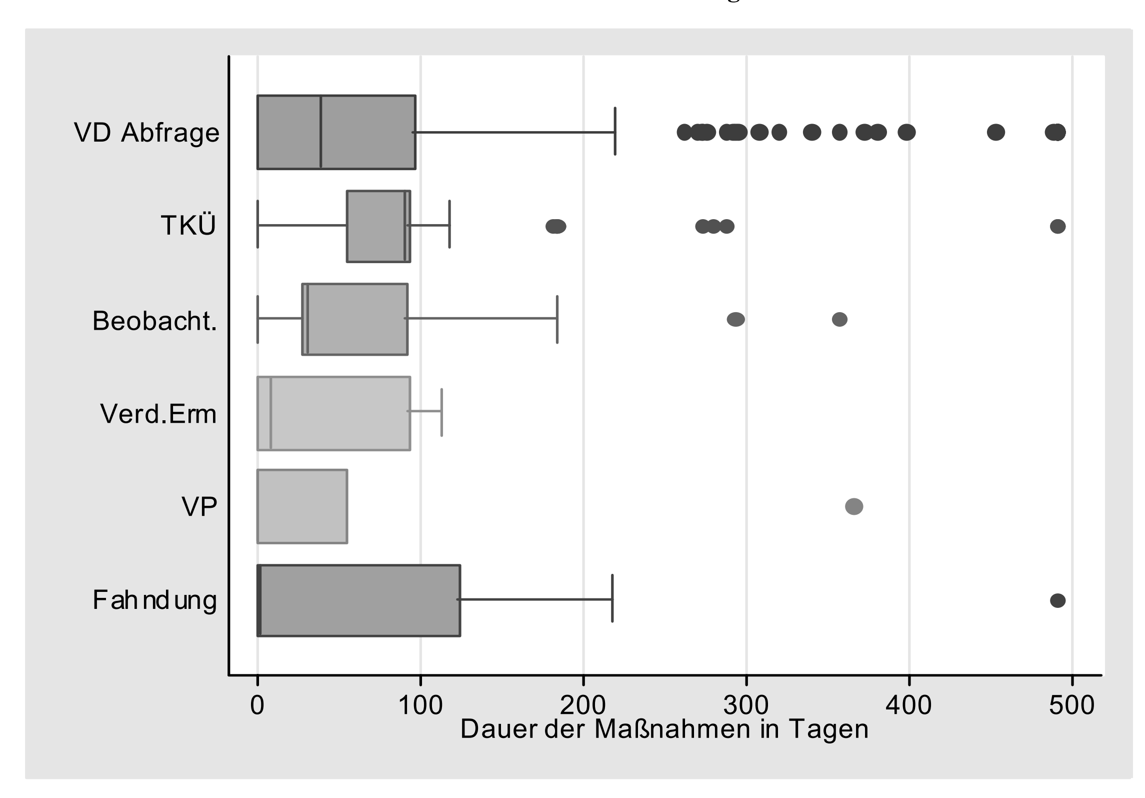
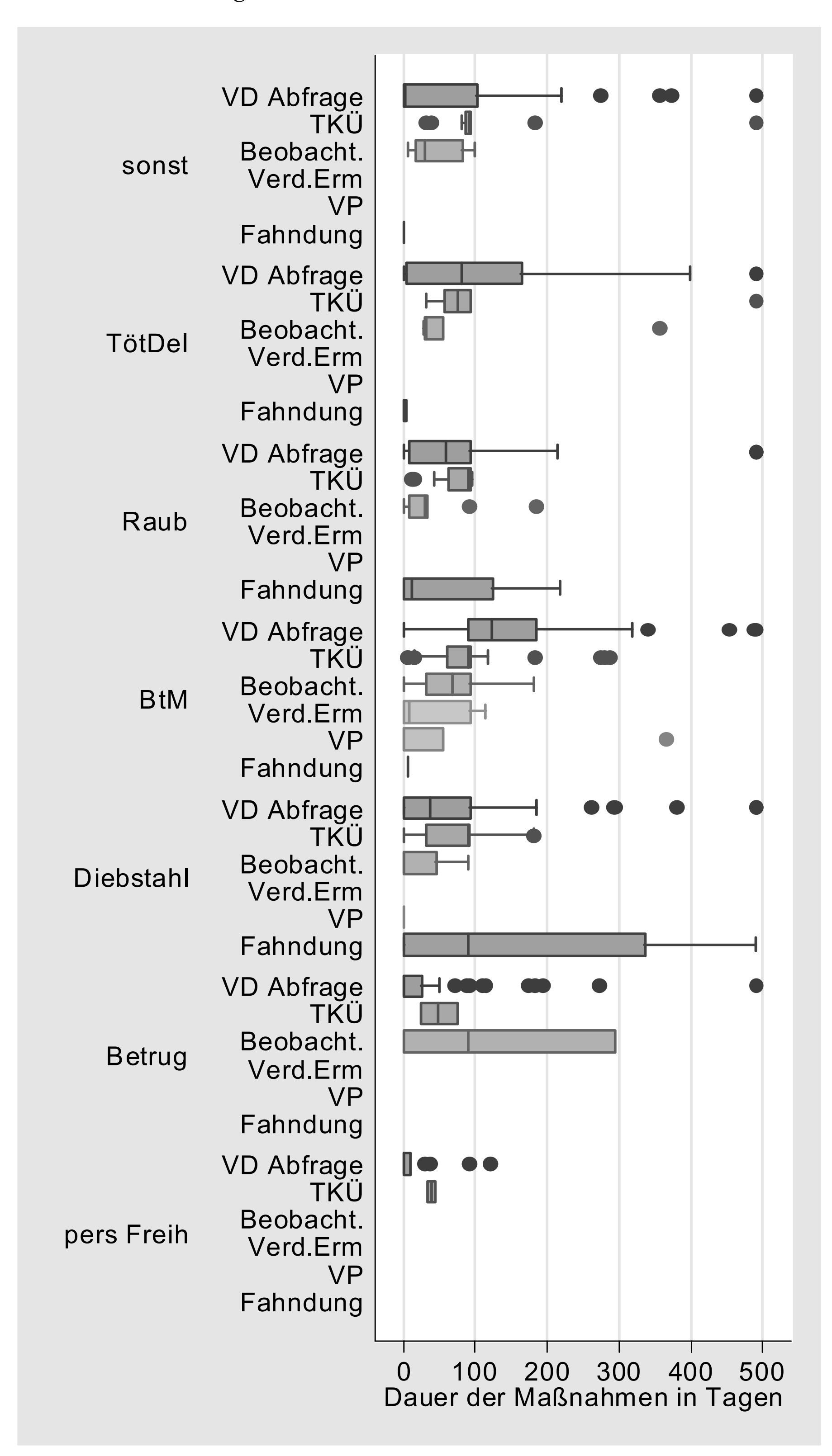


Abbildung 109

Dauer der eingesetzten Maßnahmen differenziert nach Delikten



III. Experteninterviews

1. Polizeibeamte

a) Bedeutung der Verkehrsdatenabfrage im Verhältnis zur Telekommunikationsüberwachung

Hinsichtlich ihrer Bedeutung für das Ermittlungsverfahren wurden Maßnahmen nach §§ 100a, 100b StPO im Verhältnis zu Maßnahmen nach §§ 100g, 100h StPO von den meisten befragten Polizeibeamten als gewichtiger angesehen. §§ 100a, b StPO seien wesentlich bedeutsamer, weil sie aktuelle Informationen lieferten und nicht nur retrograde Daten. Die Abfrage der Daten sei ein Ermittlungsansatz, um einen Verdacht zu verdichten. Dann ordne man §§ 100a, 100b StPO an, um eine Gruppenbildung festzustellen. §§ 100g, 100h StPO dienten also zur Vorbereitung der Telefonüberwachungsmaßnahme, nämlich um festzustellen, wer welche Anschlüsse benutze. Die Telekommunikationsüberwachung würde schließlich auch die Verkehrsdaten mit sich bringen und man bekäme darüber hinaus den Inhalt. Verkehrsdaten würden nur etwas über Telefone sagen, nicht über Personen. Ein Standortnachweis sei nur bei Daten in Verbindung mit der Stimme des Täters erbracht. Die Verkehrsdatenabfrage liefere nur Daten auf Papier. Beide Maßnahmen würden sich aber ergänzen. Nach §§ 100g, 100h StPO seien auch die zurückliegenden Daten ermittelbar und so ein Nachweis möglich, ob der Täter zu einem gegebenen Zeitpunkt telefoniert habe. §§ 100g, 100h StPO seien auch dann von Bedeutung, wenn §§ 100a, 100b aus rechtlichen Gründen nicht angeordnet werden können. §§ 100a, 100b StPO würden eine Katalogtat voraussetzen, während §§ 100g, 100h StPO auch bei anderen Straftaten einschlägig seien. Dadurch werde ein gewisser Spielraum eröffnet. Von einem Befragten wurde darauf verwiesen, dass es sich um völlig unterschiedliche Ansätze handle, die in ganz unterschiedlichen Fallkonstellationen angewendet würden. Man bringe dadurch unterschiedliche Dinge in Erfahrung. Die Telekommunikationsüberwachung sei vor allem bei organisierter Kriminalität und Betäubungsmitteln bedeutsam, während §§ 100g, 100h StPO bei Kapitalverbrechen eine wichtige Rolle spielen würden. Es wurde auch bemerkt, dass es derzeit mehr Maßnahmen nach §§ 100g, 100h StPO als solche nach §§ 100a, 100b StPO gebe. §§ 100a, 100b StPO seien zwar effektiver, aber dafür eingriffsintensiver. Es werde immer abgewogen, ob man auch den Kommunikationsinhalt brauche. Mehrere Befragte sind der Ansicht, dass die Maßnahmen dieselbe Bedeutung hätten. Eine Priorität könnte nicht zugeordnet werden. §§ 100g, 100h StPO seien oft vorbereitende Maßnahmen für §§ 100a, 100b StPO. Der Ansatz sei ebenso bedeutsam, da auf diesem Wege erst eine erfolgversprechende Telekommunikationsüberwachung durchgeführt werden könne. Die Maßnahmen ließen sich nicht voneinander trennen. Die Aufzeichnung der Gespräche sei ohne die Kenntnis, wer mit wem telefoniert habe, weniger aussagekräftig. Weiter wurde angeführt, dass nur mit §§ 100g, 100h StPO Daten zum Zeitpunkt vor und während der Tat erhoben werden können. §§ 100a, 100b StPO seien erst für in der Zukunft anfallende Daten von Bedeutung. Es sei ohne Berücksichtigung vergangener Kommunikation kaum eine aussichtsreiche Maßnahme nach §§ 100a, 100b StPO denkbar.

Fast alle befragten Polizeibeamten gaben an, dass die Verkehrsdatenabfrage bei Anordnung einer Telekommunikationsüberwachung in der Regel mit beantragt bzw. angeordnet werde. Das sei Standard, damit beide Typen von Informationen gesichert werden könnten. Insbesondere bei rückwirkender Datenerhebung würden „Kombibeschlüsse“ beantragt. Dagegen brauche man keinen Beschluss nach §§ 100g, 100h StPO, wenn eine Maßnahme nach §§ 100a, 100b StPO geschaltet sei. Dann würden die Verkehrsdaten mit übertragen. Zwei Befragte verneinten die Frage. Dies würde nicht mehr gemacht, da seit Einführung der §§ 100g, 100h StPO auch die zukünftigen Daten erfasst würden. Diese würden aber mit den Telefonüberwachungsprotokollen online geliefert. Ab und zu würden dann für zurückliegende Daten Maßnahmen nach §§ 100g, 100h StPO beantragt.

b) Bedeutung der Verkehrsdatenabfrage im Verhältnis zu anderen Maßnahmen

Die befragten Polizeibeamten sollten ggf. vorhandene Vorzüge der Verkehrsdatenabfrage im Verhältnis zu anderen Ermittlungsmaßnahmen aufführen. Ein Vorzug der Verkehrsdatenabfrage sei u. a., dass objektive Daten erhoben werden. Die Verkehrsdaten hätten einen nahezu objektiven Beweiswert. Es sei ein technisches Mittel und es gebe keine Manipulationsmöglichkeiten seitens der Täter. Es könne nicht mehr in Zweifel gezogen werden, dass kommuniziert worden sei. Es gebe deshalb auch keine Wahrnehmungsprobleme wie bei Zeugenaussagen. Das gesprochene Wort dagegen sei in unterschiedliche Richtungen zu interpretieren. Zudem würden die Daten durch unbeteiligte Dritte, die Netzbetreiber, gespeichert. Dementsprechend sei der Beweiswert höher. Man könne relativ sicher das Umfeld einer verdächtigen Person zeitnah feststellen. Über die Häufigkeit von Anrufen könne man Kontakte feststellen. Das sei durch keine andere Maßnahme zu erreichen. Man könne zudem im Nachhinein ein Bewegungsbild erstellen. Durch Funkzellenabfragen könne man feststellen, wo sich ein Mobiltelefon befunden habe. Eine herkömmliche Spur werde nur am Tatort hinterlassen. Mit den Verkehrsdaten könne ein Täter hingegen auch mit anderen Tatorten in Verbindung gebracht werden (z. B. bei mehreren Banküberfällen). Die Daten können nach Aussagen der Interviewten aber auch entlastende Wirkung haben. Ein weiterer Vorteil bestehe darin, dass relevante Informationen schnell und einfach erreichbar seien. Ohne personellen Aufwand könne dasselbe Ergebnis erzielt werden wie z. B. bei einer Observation. Ein ermittlungstaktischer Vorteil sei ferner, dass es sich gegenwärtig noch um Maßnahmen handle, mit denen der Täter nicht rechne. Die Daten könnten risikolos erhoben werden, da der Beschuldigte die Abfrage nicht kenne. Die Verkehrsdatenabfrage sei einerseits ein letztes Mittel, andererseits bei verschiedenen Delikten der einzige erfolgversprechende Ansatz. Denn Verkehrsdaten würden häufig die ersten Hinweise auf einen möglichen Täter geben. Es handle sich um eine „moderne Ermittlungsmöglichkeit, die heute in einem Ermittlungsverfahren nicht mehr

wegdenkbar ist“. Drei der Befragten meinen, dass es sich um ganz unterschiedliche Maßnahmen handle. Ein Vergleich sei schwierig. Die Verkehrsdatenabfrage erweitere das Feld der Ermittlungsmöglichkeiten. Es sei immer fallbezogen, was im Einzelnen angewandt würde. Es komme darauf an, was nachgewiesen werden soll. Es werde diejenige Maßnahme genutzt, die augenblicklich Erfolg verspreche. Insgesamt ergänze die Abfrage der Verkehrsdaten viele andere Maßnahmen.

2. Staatsanwälte

a) Bedeutung der Verkehrsdatenabfrage im Verhältnis zur Telekommunikationsüberwachung

Im Verhältnis zur Telefonüberwachung werden die Daten nach §§ 100g, 100h StPO von den befragten Staatsanwälten für weniger bedeutsam gehalten. §§ 100a, 100b StPO seien Erfolg versprechender, weil auch der Inhalt festgestellt werden könne. Nur so könnten konkrete Informationen herausgefunden werden. §§ 100g, 100h StPO würden dagegen der Vorbereitung für §§ 100a, 100b StPO dienen, insbesondere zur Entscheidung, wer abgehört werden sollte. §§ 100a, 100b StPO seien manchmal Anschlussmaßnahmen, manchmal aber auch Begleitmaßnahmen. Davon unabhängig hätten die §§ 100g, 100h StPO aber eine recht große Bedeutung und würden oft zu mehr Informationen führen als z. B. Observation und Lichtbildaufzeichnungen. Tatabläufe könnten nachgezeichnet und Bewegungsprofile erstellt werden. §§ 100g, 100h StPO würden freilich einen geringeren Eingriff in die Sphäre des Betroffenen bedeuten. Außerdem würden sie auch deshalb eine Rolle spielen, weil rückwirkende Daten erlangt werden können. Weiter wurde angegeben, dass §§ 100g, 100h StPO wesentlich häufiger seien, weil die Voraussetzungen entsprechend häufiger vorliegen würden (insbesondere wegen mittels Endeinrichtung begangenen Straftaten).

Die Verkehrsdatenabfrage würde überwiegend nicht zusammen mit der Telekommunikationsüberwachung angeordnet, meinen etwa die Hälfte der befragten Staatsanwälte. Sie sei nur bei rückwirkenden Daten bedeutend. Bei zukünftigen Daten würden die Daten ohnehin mit dem Protokoll der Telefonüberwachung übermittelt. Die übrigen Befragten geben an, dass die Maßnahmen (fast) immer gleichzeitig beantragt würden. Dies sei vor allem bei Betäubungsmitteln und organisierter Kriminalität die Regel. §§ 100g, 100h StPO würden dann nicht in die Zukunft gerichtet angewandt, weil diese Informationen mit der Telefonüberwachung erlangt werden könnten. Bei schweren Delikten würde i. d. R. eine Telefonüberwachung in die Zukunft und §§ 100g, 100h StPO in die Vergangenheit angeordnet. Bei allgemeinen Sachen ordne man dagegen nur §§ 100g, 100h StPO an.

b) Bedeutung der Verkehrsdatenabfrage im Verhältnis zu anderen Maßnahmen

Vorteil der Verkehrsdatenabfrage gegenüber anderen Ermittlungsmaßnahmen ist nach Angaben von einigen Staatsanwälten, dass es sich um eine verdeckte Maßnahme handle, die keine Außenwirkung entfalte (z. B. im Vergleich zur Durchsuchung). Es handle sich um einen relativ geringfügigen Eingriff für die Betroffenen. Ein weiterer Vorteil sei, dass man objektive Daten bekomme. Man könne Strukturen ermitteln, Täter identifizieren und Tatorte nachweisen. Die Standortkennung stehe im Vordergrund. Überall, wo Straftaten Telekommunikation erfordern, sei die Maßnahme unabdingbar. Die Bedeutung sei einzelfallabhängig, meinen weitere Befragte. Es werde geprüft, ob andere Möglichkeiten in Betracht kommen oder nicht. Die Maßnahmen seien nicht miteinander vergleichbar. Es seien nur Indizien für Kontakte von Personen untereinander oder für Aufenthaltsorte. Es seien aber Indizien, die die Möglichkeit zu weiteren Ermittlungen eröffnen könnten.

3. Richter

a) Bedeutung der Verkehrsdatenabfrage im Verhältnis zur Telekommunikationsüberwachung

Zum Verhältnis hinsichtlich ihrer Bedeutung für das Ermittlungsverfahren von Maßnahmen nach §§ 100g, 100h StPO im Verhältnis zu §§ 100a, 100b StPO wurde von den meisten befragten Richtern angegeben, dass §§ 100a, 100b StPO erheblich höhere Bedeutung hätten. Das beruhe darauf, dass man dabei auch die Inhalte und mehr Details erfahre. Die Telefonüberwachung erfasse auch zukünftige Verkehrsdaten. §§ 100g, 100h StPO sei eine Vorstufe, um festzustellen, wer der Anrufer war und erst dann würde eine Telefonüberwachung durchgeführt. Die Auskünfte zu den Verkehrsdaten dienten der Vorbereitung der Telefonüberwachung. Dagegen sei §§ 100g, 100h StPO in die Vergangenheit gerichtet wichtig. Weiter wird angegeben, dass weder das eine noch das andere erfolgreicher sei. Beim Raub von Mobiltelefonen hätten §§ 100g, 100h StPO eine größere Bedeutung, bei Betäubungsmitteln dagegen die §§ 100a, 100b StPO. Durch das Abhören könne beispielsweise nicht in Erfahrung gebracht werden, wo sich der Beschuldigte aufgehalten habe. Bei der Telefonüberwachung werde das Gespräch mitgehört, bei §§ 100g, 100h StPO könne dagegen nur gesagt werden, dass telefoniert worden sei. Ganz generell hätten die Maßnahmen nach §§ 100g, 100h StPO größere Bedeutung bei nachträglicher Betrachtung von Vorgängen, diejenigen gemäß §§ 100a, 100b StPO dagegen bei laufenden oder in die Zukunft reichenden Vorgängen.

Die Frage, ob die Maßnahme nach §§ 100g, 100h StPO bei einer Telekommunikationsüberwachung in der Regel mitbeantragt bzw. angeordnet würde, bejahten etwa die Hälfte der befragten Richter. Einzelne Staatsanwälte würden dazu übergehen, beides gleichzeitig zu beantragen. Ein Befragter weist darauf hin, dass die Anordnungen nicht in einem Beschluss ergingen, aber zeitgleich. Zwei Befragte sind der Ansicht, dass dies überflüssig sei, da die Daten von § 100a StPO miterfasst würden; die Telefonüberwachungsprotokolle würden die Verkehrsdaten mitliefern. Die Stimme sei bedeutsamer als die Information, wer formal der Inhaber eines Anschlusses ist. Ein weiterer Richter gibt an, dass die Beurteilung vom Einzelfall abhängig sei. Es müssten konkrete Anhaltspunkte

dafür vorliegen, dass die Maßnahme für die weiteren Ermittlungen erheblich ist.

b) Bedeutung der Verkehrsdatenabfrage im Verhältnis zu anderen Maßnahmen

Auch die befragten Richter gaben unterschiedliche Vorzüge der Verkehrsdatenabfrage gegenüber anderen Ermittlungsmaßnahmen an. Vorzug der Verkehrsdatenabfrage sei, dass die Maßnahme nicht so personalintensiv und nicht so aufwendig sei, außer es handle sich um große Datenmengen. Die Verkehrsdatenabfrage sei einfacher als z. B. eine Observation. Die Daten seien „vom Schreibtisch aus zu lesen“, die „Daten werden vom Anbieter serviert“. Dagegen entstünde bei großen Datenmengen eine erhebliche Arbeitsbelastung für die Polizei. Zudem handle es sich um objektivierbare Daten, während ein V-Mann beispielsweise subjektive Einschätzungen liefere. Aussagen und Urkunden könnten anhand der Daten überprüft werden. Zudem seien Anhaltspunkte für Aufenthaltsorte zu erlangen. Ein ganz entscheidender Vorteil sei außerdem die Heimlichkeit der Maßnahme. Der Beschuldigte habe in der Regel keine Kenntnis von der Maßnahme. Es sei eine „stille“ Ermittlung. Eine Durchsuchung und Beschlagnahme von Verkehrsdaten sei dagegen zu auffällig. Es gebe Fälle, in denen die Verkehrsdaten den einzig möglichen Ermittlungsansatz enthielten. Ferner könnten Kommunikationsbewegungsbilder erstellt und Netzwerke identifiziert werden. Das sei durch andere Maßnahmen nicht möglich. Das sieht ein anderer Befragter etwas skeptischer. Die Verkehrsdatenabfrage sei zwar ein wichtiger Ermittlungsansatz, von generellen Vorzügen gegenüber anderen Maßnahmen würde er aber nicht sprechen wollen. Die anderen Ermittlungsmethoden zielten auf andere Beweismittel ab. Was man mit §§ 100g, 100h StPO erreichen könne, könne man nicht mit den anderen Maßnahmen erreichen und genauso sei es mit den anderen Methoden.

4. Verteidiger

Die befragten Verteidiger gaben übereinstimmend an, dass die §§ 100a, 100b StPO für das Verfahren eine größere Rollen spielten als die §§ 100g, 100h StPO. Ein Befragter führte aus, dass sich die Verkehrsdatenabfragen oft erst aus den Maßnahmen nach §§ 100a, 100b StPO ergeben würden, jedoch könnten die Daten auch eine Telekommunikationsüberwachung nach sich ziehen. Die beiden Maßnahmen gingen oft miteinander einher, gab ein anderer Befragter an. Es würde alles auf einmal angeordnet, um „sicher zu gehen“. Es herrsche eine gewisse Unsicherheit der Gerichte, was unter welche Norm falle. In der Hauptverhandlung würden oft nur die Ergebnisse der Telekommunikationsüberwachung mit einfließen, da der Richter damit umgehen könne. §§ 100g, 100h StPO seien eher im Ermittlungsverfahren wichtig.

IV. Zusammenfassung der Ergebnisse

Die Verkehrsdatenabfrage wird sehr häufig direkt zu Beginn des Ermittlungsverfahrens eingesetzt. Dies ergibt sich aus der Analyse der Strafverfahrensakten und wird durch die Einschätzung der Befragten, dass die Abfrage der Daten meist früher als andere Ermittlungsmaßnahmen oder früher bzw. zeitgleich mit der Telekommunikationsüberwachung erfolgt, bestätigt. Den Akten war zu entnehmen, dass die Verkehrsdatenabfrage am häufigsten einen bis zwei Tage nach Beginn des Ermittlungsverfahrens eingesetzt wird. Zumindest wird der erste Beschluss aber in 51 Prozent der Fälle innerhalb der ersten 14 Tage erlassen. In 64 Prozent der untersuchten Verfahren war die Verkehrsdatenabfrage zudem der Anlass für die erste Einschaltung der Staatsanwaltschaft. Gerade bei Tötungsdelikten und Betrugsdelikten wurde die Verkehrsdatenabfrage im Vergleich zu anderen Maßnahmen sehr früh im Ermittlungsverfahren angewandt.

Kombinationen mit anderen Ermittlungsmaßnahmen erfolgen – nach Angabe der schriftlich Befragten – vor allem mit der Telekommunikationsüberwachung, aber auch mit der Durchsuchung und der Beschlagnahme. Auch im Rahmen der Expertengespräche konnte festgestellt werden, dass die Verkehrsdatenabfrage und die Telekommunikationsüberwachung häufig zusammen angeordnet werden. Die Bedeutung der Verkehrsdatenabfrage wird von den meisten interviewten Praktikern als geringer beurteilt als die der Telekommunikationsüberwachung. Oftmals würden sich die Maßnahmen jedoch ergänzen. Mit der Verkehrsdatenabfrage würden die in der Vergangenheit liegenden Daten festgestellt werden. Die Telekommunikationsüberwachung erfasse dann die zukünftigen Verkehrsdaten sowie den Inhalt der Gespräche. Geschildert wurde auch, dass die Verkehrsdatenabfrage des Öfteren zur Vorbereitung einer Telekommunikationsüberwachung durchgeführt werde. Die zu überwachenden Anschlussnummern würden in diesen Fällen mit der Verkehrsdatenabfrage ermittelt und danach werde die Telekommunikationsüberwachung geschaltet. In die Zukunft gerichtete Verkehrsdatenabfragen sind nach Ansicht der meisten Befragten bei gleichzeitiger Telekommunikationsüberwachung sinnlos, da sich die Daten bereits aus den Telekommunikationsüberwachungsprotokollen ergeben. Des Öfteren wurde auch angegeben, dass es sich bei der Verkehrsdatenabfrage oft um das einzige Mittel handele, um einen ersten Ansatz zu bekommen und danach ggf. weitere Ermittlungsmaßnahmen durchzuführen. Häufigere Kombinationen mit Durchsuchung und Beschlagnahme werden ebenfalls durch die Ergebnisse der Interviews bestätigt. Teilweise wurde angegeben, dass zunächst mit der Verkehrsdatenabfrage Verdächtige identifiziert und sodann deren Wohnungen durchsucht und ggf. vorliegende Beweise (wie Drogen) beschlagnahmt würden. In den der Aktenanalyse zugrunde liegenden Verfahren wurden neben der Verkehrsdatenabfrage ebenfalls häufig Durchsuchungen (40 Prozent der Verfahren) sowie Zeugenvernehmungen (70 Prozent), Anschlussinhaberfeststellungen nach dem Telekommunikationsgesetz (25 Prozent) sowie Telekommunikationsüberwachungsgesetzes (24 Prozent) durchgeführt.

Bei den Verfahren, in denen die Verkehrsdatenabfrage als einzige Ermittlungsmaßnahme durchgeführt wurde

(31 Verfahren), handelte es sich vor allem um Betrugsdelikte, insbesondere um den sog. Enkeltrick. Häufiger waren auch besonders schwere Fälle des Diebstahls, in denen Mobiltelefone aus aufgebrochenen Kraftfahrzeugen gestohlen wurden. Im Übrigen handelte es sich meist um mittels Endeinrichtung begangene Straftaten.

Vorzüge der Verkehrsdatenabfrage gegenüber anderen Ermittlungsmaßnahmen sind nach der Angabe der interviewten Praktiker u. a. die Objektivität der Daten und die fehlenden Manipulationsmöglichkeiten. Zudem sei von Vorteil, dass es sich um eine verdeckte Maßnahme handle und dass der Eingriff relativ geringe Arbeitsbelastung auslöse. Als Vorteil wurde von den befragten Staatsanwälten und Richtern auch angesehen, dass die Daten für sie einfach zu beschaffen und leicht auszuwerten seien – außer bei größeren Datenmengen.

E. Effizienz der Verkehrsdatenabfrage

Im dritten Teil der Arbeit soll die Effizienz der Verkehrsdatenabfrage untersucht werden. Dazu ist zunächst zu bestimmen, was unter dem Begriff der Effizienz zu verstehen ist. Die so aufgestellten Grundsätze sind dann auf den Untersuchungsgegenstand zu übertragen und die Kriterien herauszukristallisieren, aus welchen die Effizienz der Maßnahme abzuleiten ist.

I. Begriff der Effizienz und Übertragung auf den Untersuchungsgegenstand

1. Begriff der Effizienz

Die Begriffe Effizienz und Effektivität werden häufig synonym verwandt.[462] Es handelt sich dabei jedoch nach *Schroller*[463] um „Einzelaspekte einer Leistungsbeschreibung“. Unter dem Begriff der Effektivität versteht man allgemein die Wirksamkeit und die Leistungsfähigkeit des Untersuchungsgegenstandes[464]. Der Begriff betrifft die grundsätzliche Eignung einer Maßnahme, ein angestrebtes Ziel zu erreichen[465]. Mit Effizienz ist dagegen das Verhältnis zwischen Mitteleinsatz und Zielerreichung gemeint (Ziel-Mittel-Verhältnis/Input-Output-Verhältnis)[466]. *Schroller*[467] führt dazu aus, dass Maßnahmen Zielvorstellungen enthalten und um diese Ziele erreichen zu können, Mittel aufgewendet werden müssten (Input). Wenn die Maßnahmen getroffen werden, zeigen sich Wirkungen der Maßnahmen (Output). Eine Bewertung der Effizienz werde dann möglich, wenn geklärt wird, ob der Aufwand (Input) in einem vernünftigen Verhältnis zum Ertrag (Output) stand.

[462] *Büchler*, S. 33; *Schroller*, in: BKA, Symposium: Der polizeiliche Erfolg, S. 28.
[463] *Schroller*, in: BKA, Symposium: Der polizeiliche Erfolg, S. 28.
[464] *Brockhaus*, Bd. 6 S. 113.
[465] *Büchler*, S. 33.
[466] *Büchler*, S. 33; *Brockhaus*, Bd. 6 S. 114.
[467] *Schroller*, in: BKA, Symposium: Der polizeiliche Erfolg, S. 29.

2. Übertragung auf den Untersuchungsgegenstand

Gegenstand der vorliegenden Arbeit ist die Evaluation der Effizienz der Ermittlungsmethode nach §§ 100g, 100h StPO. Dazu sind zunächst die Ziele der Verkehrsdatenabfrage zu bestimmen, die mit der Maßnahme erreicht werden sollen. Die Mittel, die dazu aufgewendet werden, sind zum einen die Eingriffe in die Grundrechte der Betroffenen und zum anderen der Aufwand und die Kosten, die durch die Abfrage der Daten bei den Telekommunikationsanbietern und den übrigen Beteiligten entstehen.

Die Wirkungen der Maßnahmen und damit die Effizienz wurden in verschiedener Hinsicht erfasst. Im Rahmen der Aktenanalyse wurden zum einen allgemeine Erfolgseinschätzungen, die der Akte zu entnehmen waren oder die der jeweilige Bearbeiter der Akte abgeben konnte, aufgenommen. Dabei wurde bei der Beurteilung des Erfolges unterschieden, ob die Maßnahmen für den jeweiligen betroffenen Anschluss, den gesamten Beschluss, den jeweiligen Beschuldigten und für das Verfahren insgesamt erfolgreich, bedingt erfolgreich oder nicht erfolgreich waren.

Zum anderen wurden auch die spezifischen Erfolge aufgenommen. Anhand der Akten konnte festgestellt werden, welche konkreten Erfolge erzielt werden. Dabei sind beschlussbezogene, beschuldigtenbezogene und verfahrensbezogene Erfolge zu unterscheiden. Je nachdem, welche Informationen den Akten zu entnehmen waren, wurde für jeden Beschluss, für jeden Beschuldigten und für jedes Verfahren der konkret eingetretene Erfolg aufgenommen.

Mit der Verkehrsdatenabfrage können nie direkte, d. h. unmittelbare Erfolge erzielt werden. Die Abfrage der Daten lässt immer nur Aussagen darüber zu, ob sich z. B. ein bestimmtes Mobiltelefon an einem bestimmten Ort befunden hat. Es ist nicht möglich, dem Täter direkt nachzuweisen, dass er sich z. B. zur Tatzeit in der Nähe des Tatorts befunden hat. Man kann nur Aussagen z. B. über das Mobiltelefon treffen. Es kann nachgewiesen werden, dass von dem Anschluss des Inhabers aus der bedrohende Anruf ausging, aber nicht, ob der Anschlussinhaber auch tatsächlich derjenige war, der die Drohung geäußert hat. Es handelt sich demnach um Indizien, die in Verbindung mit anderen Beweismitteln aber Beweiskraft entfalten können.

Bei diesen indirekten Erfolgen sind verschiedene Wirkungen zu unterscheiden. Zum einen kann die Verkehrsdatenabfrage zur Identifizierung des Täters bzw. des Verdächtigen beitragen. Dass ist z. B. der Fall, wenn das Opfer von einem bestimmten Anschluss angerufen und (z. B.) bedroht wurde und der Anschlussinhaber mit Hilfe der Datenabfrage identifiziert werden kann. Ein weiterer Erfolg ist die Identifizierung weiterer Anschlüsse des Beschuldigten, die dann ebenfalls einer Verkehrsdatenabfrage oder Telekommunikationsüberwachung unterzogen werden können. Auf diese Weise können die Ermittlun-

gen vorangetrieben werden. Des Weiteren ist es möglich, den Standort des überwachten Handys zur Tatzeit zu bestimmen. Wiederum sind zwar keine Aussagen darüber möglich, ob wirklich der Beschuldigte am Tatort war, aber zusammen mit anderen Beweismitteln wie einer Zeugenaussage oder eines dadurch erwirkten Geständnisses entfaltet die Datenabfrage eine Beweiswirkung. Zudem kann die Tatzeit bestimmt bzw. eingegrenzt werden, indem Datum und Uhrzeit einer Verbindung zu einem bestimmten Anschluss abgefragt werden. Wenn ein Mobiltelefon benutzt wird, kann nachträglich und auch für die Zukunft ein Bewegungsbild erstellt werden. Man kann feststellen, wann sich eine Rufnummer in welche Funkzelle eingewählt hat. Ebenso ist es möglich, einen Beschuldigten durch die Verkehrsdatenabfrage zu entlasten. Behauptet etwa ein vermeintliches Stalking-Opfer, dass es von einem bestimmten Anschlussinhaber angerufen wurde, lässt sich dies anhand der Daten feststellen oder entkräften. Auf dem gleichen Wege lässt sich auch die Glaubhaftigkeit einer Aussage bestätigen oder widerlegen, auch was eventuelle Standortangaben betrifft. Unterstützen lässt sich mit der Maßnahme zudem eine Erweiterung des Tatvorwurfs, wenn sich im Zusammenhang mit andren Beweismitteln Hinweise auf weitere Straftaten ergeben. Kommunikationspartner des Beschuldigten können nachgewiesen werden, indem die abgehenden und eingehenden Anrufe von und zur Rufnummer des Beschuldigten abgefragt werden. Daraus können sich auch – wiederum mittelbar mit anderen Hinweisen – die Tatbeteiligung der Kommunikationspartner und Hinweise auf eventuelle weitere Straftaten ergeben. Die Verkehrsdatenabfrage kann zur Feststellung von Rufnummern, IMEI-Nummern und IP-Adressen für eine Folge-Maßnahme nach §§ 100g, 100h StPO führen, wodurch die Ermittlungen weiter vorangetrieben werden können. In die gleiche Richtung geht die Feststellung, ob andere Ermittlungsmaßnahmen, z. B. die Telefonüberwachung, erfolgversprechend sein könnten. Zudem kann die Verkehrsdatenabfrage allgemein zur Sicherung von Beweisen dienen und zusammen mit anderen Beweismitteln zur Aufklärung beitragen.

Von den Erfolgen, die mit der Verkehrsdatenabfrage im Ermittlungsverfahren erreicht werden können, sind diejenigen zu unterscheiden, die außerhalb des Ermittlungsverfahrens eingetreten sind. So kann die Effizienz daran gemessen werden, ob Anklage erhoben und der Angeklagte auch verurteilt wurde und ob dies im Zusammenhang mit dem Erfolg der Verkehrsdatenabfrage steht. Weiter ist unter dem Gesichtspunkt der Effizienz zu überprüfen, ob die Abfrage der Verkehrsdaten als Beweismittel in der Anklage bedeutsam war, welche Rolle die Verkehrsdaten in der Hauptverhandlung gespielt haben und welcher Stellenwert ihnen bei der Beweiswürdigung im Rahmen des Urteils zukam.

Bei den Interviews und der schriftlichen Befragung wurden die Befragten allgemeiner dazu befragt, welche Ziele mit der Verkehrsdatenabfrage verfolgt werden und welche Erfolge ihrer Erfahrung nach eintreten bzw. eingetreten sind. Zudem wurden Fragen nach der Bedeutung der Daten für den weiteren Verfahrensverlauf gestellt.

Die Beurteilung der Effizienz beruht also auf der Kombination verschiedener Methoden und aus dem Zusammenspiel verschiedener Indikatoren. Die Beurteilung des Beitrags der Verkehrsdaten für den Ermittlungserfolg setzt auf verschiedene Perspektiven. Zum einen handelt es sich qualitative Perspektiven, die aus den Einschätzungen (oder Ratings) der Bearbeiter der Aktenauswertung, die den konkreten Verfahrensverlauf in den Ermittlungs- und Strafakten im Blick haben, und den allgemeinen Beurteilungen von Schlüsselpersonen aus dem Strafverfolgungsbereich und der Strafverteidigung gebildet werden. Diese sind ergänzt um Indikatoren, die aus den Strafakten entnommen werden können und mit bestimmten Erledigungsformen (Einstellungen gemäß § 170 II 2 StPO), Vermerken zum Erfolg in den Akten bzw. entsprechende Nennungen in Anklage und Urteilsgründen verbunden sind.

II. Ziele der Verkehrsdatenabfrage

Zunächst wurden die Ziele, die mit der Verkehrsdatenabfrage verfolgt werden, durch die verschiedenen Module erfasst.

1. Schriftliche Befragung

Die Ziele, die nach Angaben der Befragten mit der Verkehrsdatenabfrage verfolgt werden, sind in Tabelle 26 aufgeführt.

Als kriminalistische Ziele bei einer Verkehrsdatenabfrage werden häufig die Identifizierung des Beschuldigten, die Feststellung von Kommunikationspartnern des Beschuldigten und von weiteren Tatbeteiligten sowie weiteren Anschlüssen des Beschuldigten und die Erlangung von Beweismitteln genannt. Gelegentlich auftretende Ziele seien die Bestimmung des Standorts des Beschuldigten zur Tatzeit, die Ermittlung des aktuellen Aufenthaltsorts des Beschuldigten sowie die Überprüfung, ob eventuell eine Telekommunikationsüberwachung erfolgversprechend sein könnte. Selten spiele die Bestimmung der Tatzeit, die Feststellung, ob eine andere Ermittlungsmethode (abgesehen von der Telekommunikationsüberwachung) in Betracht kommt, sowie die Bekämpfung von Datennetzkriminalität eine Rolle.

Diese Frage wurde je nach Zugehörigkeit des Befragten zu verschiedenen Dezernaten unterschiedlich beantwortet. Nicht vom Dezernat abhängig waren die Bestimmung des Standortes des Beschuldigten zur Tatzeit sowie die Bestimmung der Tatzeit. Ebenso waren die Einschätzung, welche Rolle die Erlangung von Beweismitteln spiele sowie die Klärung der Frage, ob eine andere Ermittlungsmaßnahme abgesehen von einer Telekommunikationsüberwachung in Betracht kommt, nicht vom Dezernat abhängig.

Tabelle 26

Kriminalistische Ziele der Auskunftserteilung (Angaben in Prozent)

	Nie	selten	gelegentl.	häufig	I immer	k.A.
Identifizierung des Beschuldigten	*1,3*	*5,8*	*14,0*	***52,7***	*13,5*	*12,7*
Feststellung von Kommunikations-partnern des Beschuldigten	*2,5*	*6,3*	*21,2*	***47,0***	*7,1*	*15,9*
Feststellung weiterer Tatbeteiligter	*2,2*	*7,8*	*25,2*	***43,2***	*4,1*	*17,5*
Feststellung von (weiteren) Anschlüssen des Beschuldigten	*5,4*	*15,9*	*23,9*	***31,4***	*2,7*	*20,7*
Erlangung von Beweismitteln	*5,0*	*15,0*	*20,7*	***30,4***	*9,7*	*19,1*
Bestimmung des Standorts des Besch. zur Tatzeit	*3,5*	*18,3*	***31,0***	*26,1*	*2,5*	*18,4*
Ermittlung des aktuellen Standorts des Beschuldigten	*8,1*	*26,9*	***29,4***	*13,7*	*0,8*	*21,1*
Feststellung, ob TKÜ erfolgver-sprechend sein könnte	*12,5*	***25,5***	***25,5***	*12,6*	*1,0*	*22,9*
Bestimmung der Tatzeit	*12,1*	***31,6***	*19,8*	*11,6*	*1,8*	*23,1*
Feststellung, ob andere Ermittlungs-maßnahme als TKÜ in Betracht kommt	*14,6*	***29,6***	*23,0*	*6,9*	*0,9*	*24,9*
Bekämpfung der Datennetz-kriminalität	*13,2*	***19,2***	*16,9*	*15,3*	*1,9*	*33,4*

2. Aktenanalyse

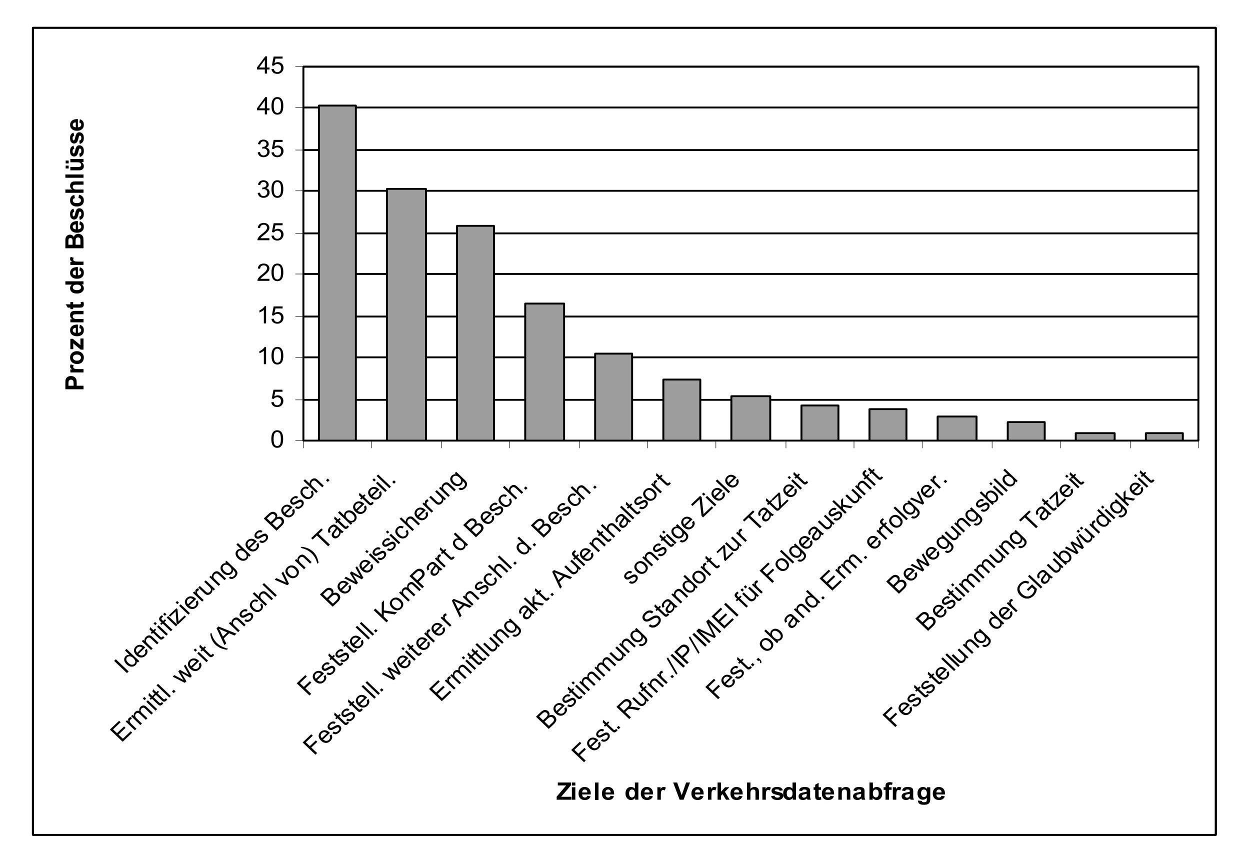
Bei der Auswertung der Akten wurden die Ziele, die mit der Anordnung der Maßnahmen nach §§ 100g, 100h StPO verfolgt wurden und den Akten zu entnehmen waren, aufgenommen. In welchem Umfang mit den Beschlüssen welche Ziele verfolgt wurden, kann Abbildung 110 entnommen werden.

Das häufigste Ziel der Verkehrsdatenabfragen war die Identifizierung des noch unbekannten Täters (40 Prozent der Beschlüsse). Die Ermittlung weiterer Tatbeteiligter bzw. ihrer Anschlüsse war in 30 Prozent der Beschlüsse Ziel der Maßnahmen. Ein häufig dokumentiertes Ziel war auch die Sicherung von Beweisen (26 Prozent). Die Feststellung der Glaubwürdigkeit des Beschuldigten oder eines Zeugen wurde eher selten verfolgt (1 Prozent). Sonstige Ziele (5 Prozent) waren u. a. die Ermittlung von Liefer- und Absatzwegen, die Ermittlung des Tatorts, die Aufhellung der Bandenstruktur, die Feststellung der Aufenthaltsorte der Mittäter, das Auffinden von geraubten Mobiltelefonen und die Ermittlung eines Zeugen.

Abbildung 110



Ziele, die mit der Verkehrsdatenabfrage verfolgt werden



3. Experteninterviews

Hinsichtlich der dezernatsspezifischen Ziele wurden die befragten Staatsanwälte um Stellungnahme gebeten. Ziele, die mit der Verkehrsdatenabfrage im Bereich organisierte Kriminalität und Betäubungsmittel verfolgt werden, seien nach Angabe der befragten Staatsanwälte die Identifizierung der Täter, die Feststellung von Täterstrukturen, der allgemeine Nachweis von Verbindungen zwischen bestimmten Personen sowie der teilweise Tatnachweis durch Standortfeststellung. Die Ermittlung weiterer Bandenmitglieder sei ein weiteres Ziel. Gerade bei Betäubungsmittelstraftaten diene die Verkehrsdatenabfrage der Feststellung von Händlern, Zwischenhändlern, Abnehmern und Handelswegen. Aufenthaltsorte von Personen (z. B. bei Beschaffungsfahrten) sollten ermittelt werden sowie die Häufigkeiten der Fahrten. Kommunikationspartner, Kontakte und Tatabläufe werden gleichfalls als Ermittlungsziele genannt.

Im Bereich der Computerkriminalität werde versucht, die Täteridentifizierung sowie den Tatnachweis mit der Abfrage der Daten zu erreichen. Bei Taten der Wirtschaftskriminalität dienten die Daten dazu, Beziehungsgeflechte festzustellen und der Klärung, wer zur Tatzeit telefoniert habe. Im allgemeinen Dezernat sei ein Hauptziel, das mit Verkehrsdaten verfolgt werde, die Identifizierung von Personen, die an Straftaten beteiligt seien.

III. Erfolge der Verkehrsdatenabfrage für die Ermittlungen

1. Schriftliche Befragung

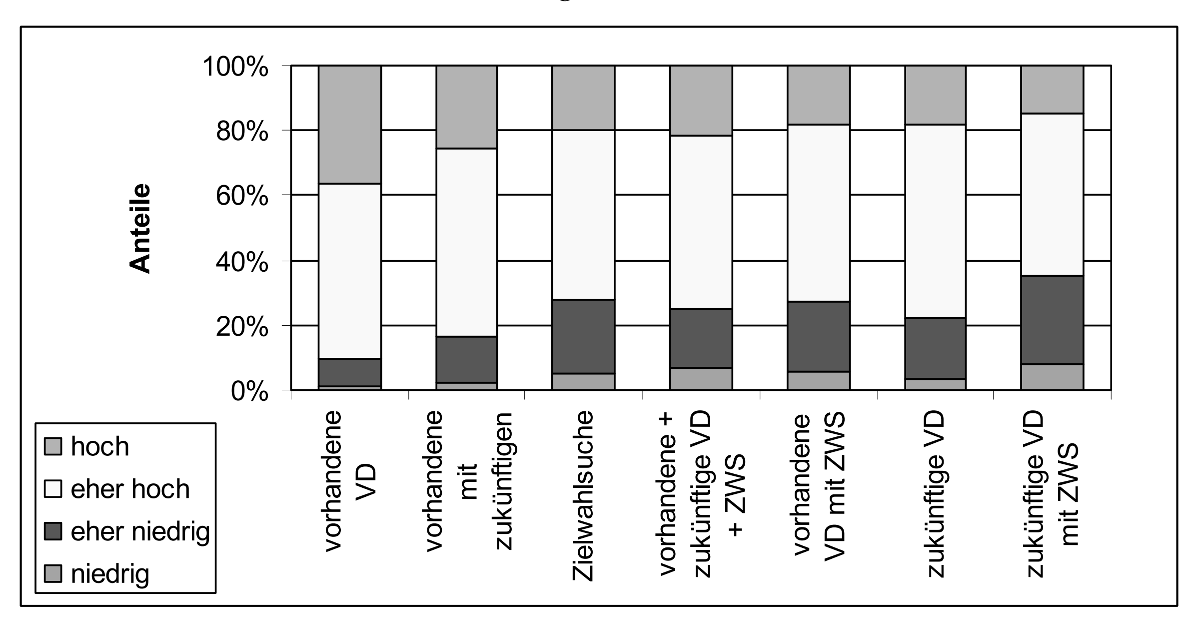
Die befragten Staatsanwälte wurden um eine allgemeine Einschätzung der Erfolgsaussichten der einzelnen Anwendungsbereiche der Verkehrsdatenabfrage gebeten.

Insgesamt wurden die Erfolgsaussichten der Verkehrsdatenabfrage eher hoch bewertet (Abbildung 111). Am erfolgreichsten wird von den Befragten die Abfrage vorhandener Verkehrsdaten eingeschätzt. Die kombinierte Abfrage vorhandener und zukünftiger Verkehrsdaten wurde diesbezüglich am zweithäufigsten genannt. Darauf folgen die alleinige Anordnung der Zielwahlsuche sowie die Kombination der drei Anwendungsbereiche. Etwas weniger erfolgreich wurde die Anwendung der Zielwahlsuche zusammen mit der Abfrage zukünftiger Verkehrsdaten sowie die alleinige Abfrage zukünftiger Daten eingeschätzt. Die geringste Erfolgsaussicht wird bei der Kombination der Zielwahlsuche zusammen mit der Abfrage zukünftiger Verkehrsdaten angenommen, wobei auch hier die Erfolgsausichten noch zum größten Teil als eher hoch bis hoch betrachtet werden.

Die Einschätzung der praktischen Bedeutung ergab ein breites Spektrum von gering (12 Prozent) über eher ge-

Abbildung 111

Erfolgsaussichten



ring (31 Prozent) und eher hoch (38 Prozent) bis zu hoch (19 Prozent). Diese Einschätzung hängt signifikant vom Dezernat ab, in dem die Befragten arbeiten. Eine (eher) hohe Bedeutung wurde der Maßnahme in den Dezernaten Internetkriminalität, organisierte Kriminalität, Kapital- und Sexualdelikte zugewiesen. Eine leicht überdurchschnittliche Bedeutung wurde auch noch seitens der Dezernenten der Betäubungsmittelabteilungen gesehen. Alle anderen Dezernate lagen unter dem Durchschnitt, wobei die geringste Bedeutung im Rahmen von Verkehrsdelikten gesehen wurde. Auf die Frage, welche Auswirkungen es hätte, wenn die Regelungen der §§ 100g, 100h StPO Ende des Jahres 2007 nicht verlängert werden würden, gaben 63 Prozent der Befragten an, dass die Maßnahmen unverzichtbar seien. 51 Prozent sind der Ansicht, dass die Verkehrsdatenabfrage nicht ersetzbar sei durch andere Ermittlungsmaßnahmen. 4 Prozent meinten, das wäre kein Verlust und 3 Prozent der Befragten waren der Meinung, dass die Auskunftserteilung durch häufigere Anwendung anderer Ermittlungsmaßnahmen, insbesondere die Telekommunikationsüberwachung, ersetzt werden könne. Weitere Antworten waren, dass Taten bei Wegfall der Vorschriften teilweise nicht aufklärbar und Täter nicht ermittelbar seien. Eine erfolgversprechende Strafverfolgung sei in vielen Bereichen ohne die Auskunft über Verkehrsdaten nicht möglich.

2. Aktenanalyse

a) Vorbemerkung

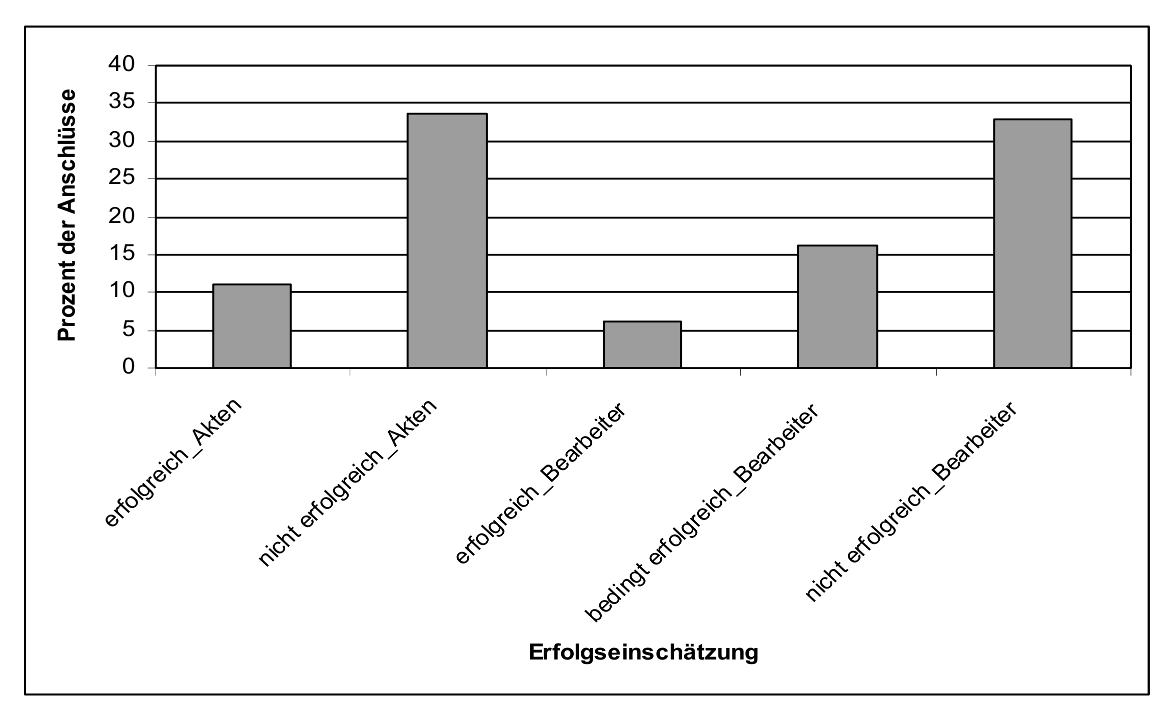
Anhand der Akten wurden über Vermerke zum Erfolg von Maßnahmen und über Ratings der Bearbeiter Feststellungen dazu getroffen, ob die Verkehrsdatenabfrage erfolgreich war und welche konkreten Erfolge mit ihr verbunden werden. Dabei sind anschlussbezogene, beschlussbezogene, beschuldigtenbezogene und verfahrensbezogene Erfolge zu unterscheiden. Je nachdem, welche Informationen den Akten zu entnehmen waren, wurde also für jede einzelne Anschlussnummer der Erfolg aufgenommen, für jeden einzelnen Beschluss, für jeden Beschuldigten und für jedes Verfahren.

b) Anschlussbezogene Erfolge

Abbildung 112 kann entnommen werden, in welchem Umfang die Verkehrsdatenabfrage in den Akten als erfolgreich bezeichnet bzw. vom jeweiligen Bearbeiter als erfolgreich eingeschätzt wurde. Bezogen auf die Anschlüsse wurde in 11 Prozent der Fälle die Verkehrsdatenabfrage in der Akte als erfolgreich bezeichnet und in weiteren 6 Prozent vom Bearbeiter als erfolgreich eingeschätzt. In 16 Prozent der Fälle schätzte der Bearbeiter die Maßnahme als „bedingt erfolgreich“ ein. Als nicht erfolgreich beurteilt wurde die Abfrage der Daten nach den Angaben in den Akten zu 34 Prozent. Bei weiteren 33 Prozent der Fälle schätzten die jeweiligen Bearbeiter die Verkehrsdatenabfrage als nicht erfolgreich ein. Damit kann die Abfrage von Verkehrsdaten bezogen auf einzelne Anschlüsse zu einem Drittel als (bedingt) erfolgreich und zu zwei Drittel als erfolglos betrachtet werden. Dazu ist anzumerken, dass trotzdem der Großteil der Beschlüsse und damit der Maßnahmen erfolgreich sein kann. Wenn beispielsweise zehn Anschlüsse durch einen Beschluss überwacht wurden und die Abfrage der Daten bzgl. eines Anschlusses davon erfolgreich war, hat die Maßnahme insgesamt zum Erfolg geführt. Die Abfrage der Daten zu den neun anderen Anschlüssen dagegen muss als nicht erfolgreich bewertet werden.

Abbildung 112

Erfolgseinschätzung bei Anschlüssen



Bezogen auf die Art des Anschlusses ergaben sich dabei signifikante Unterschiede. Die geringsten Erfolge konnten bei betrieblichen Festnetzanschlüssen erzielt werden. Dabei fällt auf, dass bezüglich des Erfolges bei den betrieblichen Festnetzanschlüssen besonders häufig Vermerke in den Akten zu finden waren. Dies mag damit zusammenhängen, dass die Eingriffsintensität bei dem Anschluss eines Betriebes aufgrund der Vielzahl der Betroffenen besonders hoch ist und deshalb auf den Erfolg oder Misserfolg besonders eingegangen wurde. Die meisten Erfolge wurden bei der Abfrage von Daten aus Telefonzellen erzielt (50 Prozent Erfolge gegenüber durchschnittlich ca. 17 Prozent).

c) Beschlussbezogene Erfolge

(1) Allgemeine Erfolgseinschätzung

Bei 43 Prozent der Beschlüsse konnte aus den Akten eine Erfolgseinschätzung entnommen werden. Von diesen Fällen wurde bei 18 Prozent der Beschlüsse die Verkehrsdatenabfrage in den Akten als erfolgreich eingeschätzt. 17 Prozent der Beschlüsse wurden in den Akten als bedingt erfolgreich und 65 Prozent als nicht erfolgreich bezeichnet.

Wenn es möglich war, notierten die Bearbeiter ihre eigenen Einschätzungen. Bei 54 Prozent der Beschlüsse war dies der Fall. Nach diesen Einschätzungen entsteht eine vergleichbare Verteilung. Bei 15 Prozent der Beschlüsse wurde die Verkehrsdatenabfrage als erfolgreich, bei 24 Prozent als bedingt erfolgreich und bei 61 Prozent als nicht erfolgreich eingeschätzt.

In Abbildung 113 wird dargestellt, wie der Erfolg insgesamt, d. h. entweder direkt aus der Akte oder nach eigener Einschätzung, beurteilt wurde. Bei 58 Prozent der Beschlüsse lag mindestens eine der beiden Einschätzungen vor. Zusammengefasst (mit Priorität für Erfolgsangaben) wird die Verkehrsdatenabfrage bei 16 Prozent der Beschlüsse in den Akten oder vom Bearbeiter als erfolgreich, bei 23 Prozent als bedingt erfolgreich und bei 61 Prozent als nicht erfolgreich beurteilt.

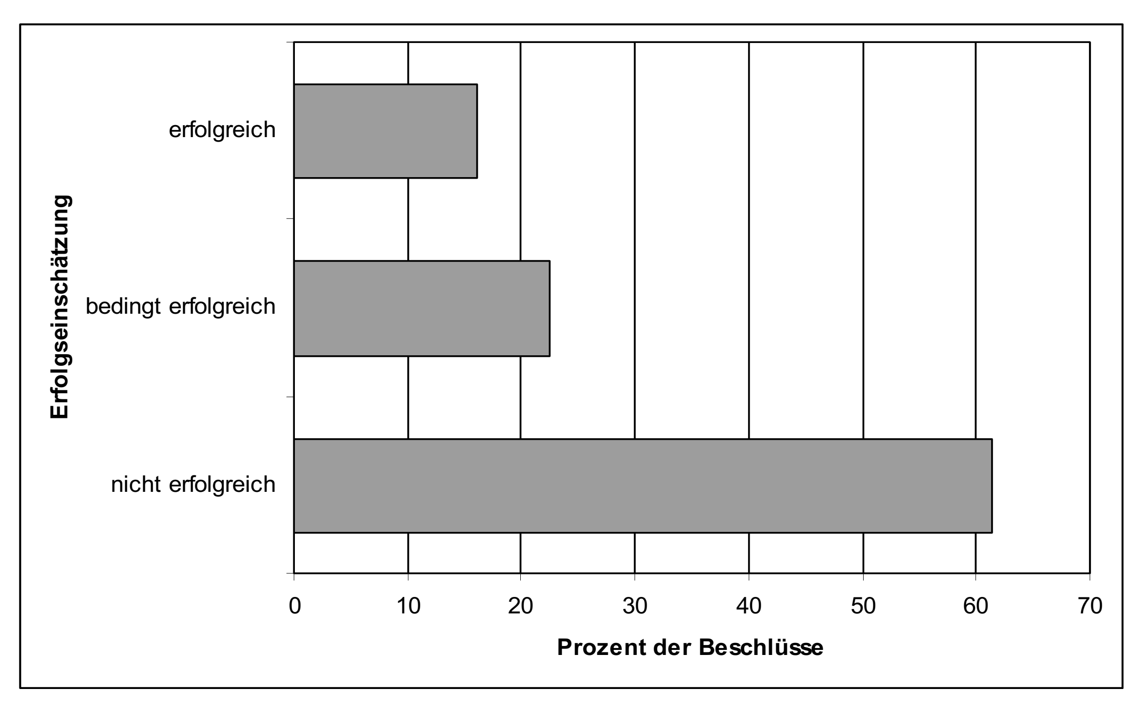
Unter der Einschränkung, dass nur bei 58 Prozent der Beschlüsse Erfolgsangaben konkret einem Beschluss zugeordnet werden konnten, bleibt als Ergebnis festzuhalten, dass etwa zwei Drittel der Beschlüsse nicht als erfolgreich bezeichnet werden können.

(2) Spezifische Erfolge der Beschlüsse

Mit der Verkehrsdatenabfrage können, wie bereits ausgeführt wurde, nie direkte Erfolge erzielt werden. Es lassen sich keine unmittelbaren Tatnachweise erbringen, sondern – zum Teil sehr aussagekräftige – Hinweise erlangen. Die bereits erläuterten spezifischen Erfolge wurden u. a. beschlussbezogen aufgenommen. In den untersuchten Akten befanden sich insgesamt 1 257 Beschlüsse. Wie bereits ausgeführt wurde, konnte den Akten teilweise

Abbildung 113

Erfolgseinschätzung der Beschlüsse



entnommen werden, welchen Beschlüssen, welche Erfolge zugeordnet werden. Bei 17 Prozent der Beschlüsse (bezogen auf alle Beschlüsse) war explizit mindestens ein spezifischer Erfolg eingetragen. In Abbildung 114 ist dargestellt, wie häufig welche Erfolge mit den Beschlüssen erzielt werden konnten.

Die am häufigsten aktenkundigen oder vom Bearbeiter festgestellten Erfolge in den Beschlüssen waren die Feststellung weiterer Tatbeteiligter (4 Prozent der Beschlüsse), die Identifizierung des Beschuldigten (3,8 Prozent), die Feststellung von Kommunikationspartnern des Beschuldigten (3,4 Prozent) sowie die Sicherung von Beweisen (2,7 Prozent).

Häufige Erfolge waren weiter die Erlangung von Hinweisen auf unbekannte Straftaten anderer (2,2 Prozent), die Feststellung von Rufnummer oder IP-Adresse für eine Folge-Auskunftserteilung (2,2 Prozent) sowie die Bestimmung des Standorts des Beschuldigten bzw. des Mobiltelefons zur Tatzeit (1,9 Prozent). Etwas weniger häufig kamen die Feststellung, ob andere Ermittlungsmaßnahmen erfolgversprechend sind (1,7 Prozent), die Erlangung von Ermittlungsansätzen für weitere Katalogstraftaten (1,5 Prozent) sowie sonstige Erfolge (1,8 Prozent) vor. Ebenso wurde die belastende Wirkung der Verkehrsdaten in Verbindung mit anderen Beweismitteln (1,5 Prozent), die Feststellung weiterer Anschlüsse des Beschuldigten (1,4 Prozent), die Erweiterung des Tatvorwurfs (1,3 Prozent) sowie die Erstellung eines Bewegungsbildes (1 Prozent) in etwas geringerem Umfang festgestellt. Die Beschlüsse führten nur selten zur Entlastung des Beschuldigten, zur Bestimmung der Tatzeit, zur Erlangung weiterer Hinweise auf sonstige Straftaten sowie zur Bestimmung des aktuellen Aufenthaltsortes des Beschuldigten.

Die Anzahl der Erfolge pro Beschluss (wenn solche genannt wurden) ist sehr schief verteilt. Am häufigsten wurde ein einzelner spezifischer Erfolg erzielt (19 Prozent der Beschlüsse). Zwei Erfolge wurden in 5 Prozent der Fälle einem Beschluss zugeordnet. In jeweils 1 Prozent wurden drei, vier, sechs und sieben spezifische Erfolge mit dem Beschluss erzielt. Diese Verteilung verändert sich nicht wesentlich, wenn die Verfahren gegen Unbekannt ausgeschlossen werden. Allerdings konnten bei den Verfahren gegen bekannte Beschuldigte etwas häufiger den Beschlüssen mindestens ein spezifischer Erfolg zugeordnet werden (20 Prozent der Beschlüsse gegenüber 17 Prozent bei allen Verfahren).

(3) Erreichte Erfolge im Vergleich zu den Zielen

Mit den Beschlüssen wurden meist konkrete Ziele verfolgt. In welchem Umfang welche Ziele erreicht wurden und in welchem Umfang andere Erfolge eingetreten sind, ergibt sich aus Abbildung 115. Das häufigste Ziel, welches aus den Akten ersichtlich war, war die Identifizierung des noch unbekannten Täters (508 Be-

Abbildung 114



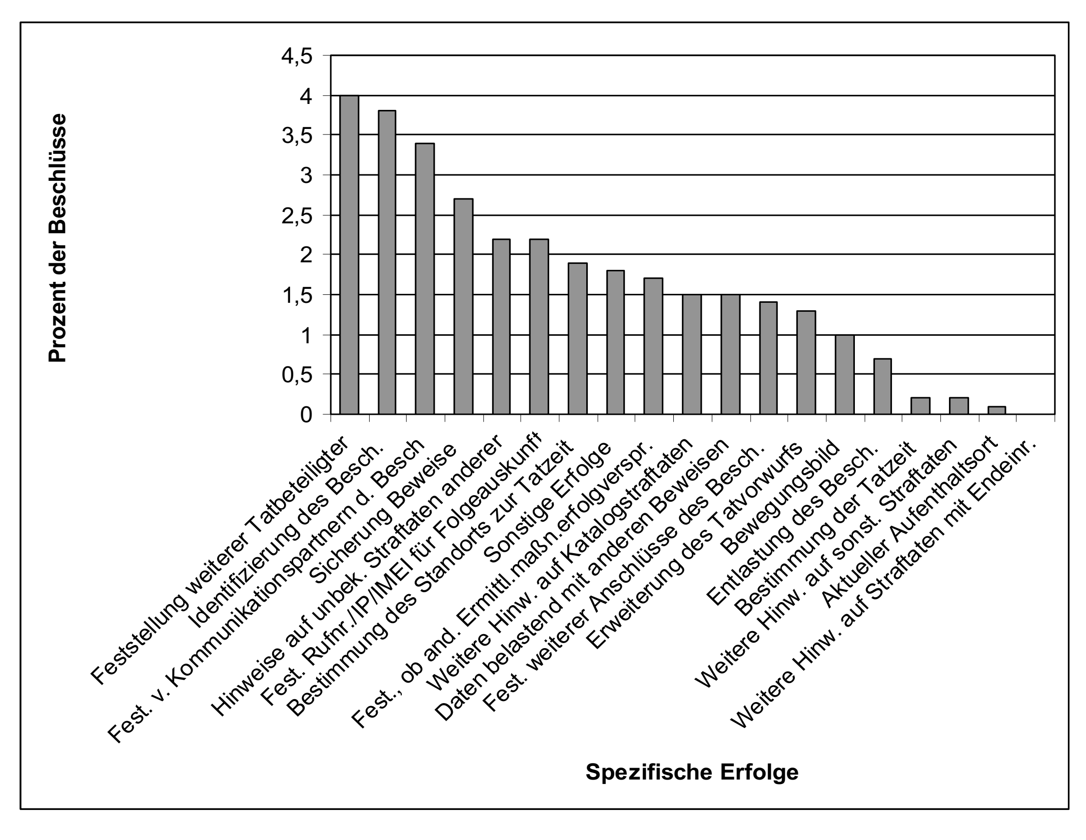
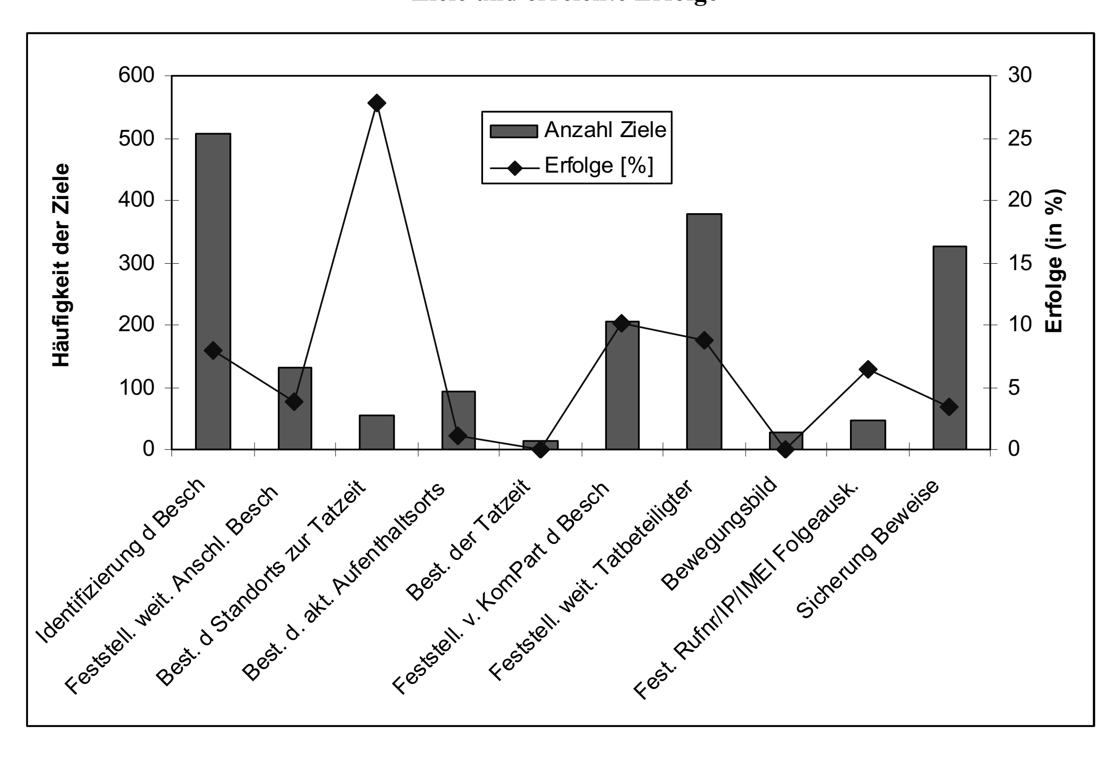


Abbildung 115

Ziele und erreichte Erfolge



schlüsse). Erreicht wurde dieses Ziel explizit allerdings nur in 8 Prozent der Beschlüsse. Häufiges Ziel war auch die Feststellung weiterer Tatbeteiligter (379 Beschlüsse), was in 9 Prozent der Beschlüsse erfolgreich umgesetzt wurde. Die Sicherung von Beweisen wurde in 325 Beschlüssen verfolgt und in 3 Prozent der Beschlüsse erreicht. Eher seltenes Ziel, aber häufig erreichter Erfolg war die Bestimmung des Standorts des Beschuldigten zur Tatzeit. In 54 Beschlüssen sollte dieses Ziel erreicht werden. Erfolgreich war es in 28 Prozent der Beschlüsse. Zu berücksichtigen ist in diesem Zusammenhang, dass oftmals das allgemeine Ziel „Identifizierung des Täters" angegeben worden sein kann, weil noch keinerlei andere Anhaltspunkte für Ermittlungen vorlagen.

Bis zu sieben Ziele wurden mit den einzelnen Verkehrsdatenabfragen verfolgt. Am häufigsten war den Akten ein Ziel pro Beschluss zu entnehmen (55 Prozent). Zwei Ziele wurden in 24 Prozent der Beschlüsse verfolgt und drei Ziele in 8 Prozent der Beschlüsse. Seltener wurden vier (4 Prozent), fünf (2 Prozent) und sieben (1 Prozent) Ziele gleichzeitig mit den Maßnahmen verfolgt.

d) Verfahrensbezogene Erfolge

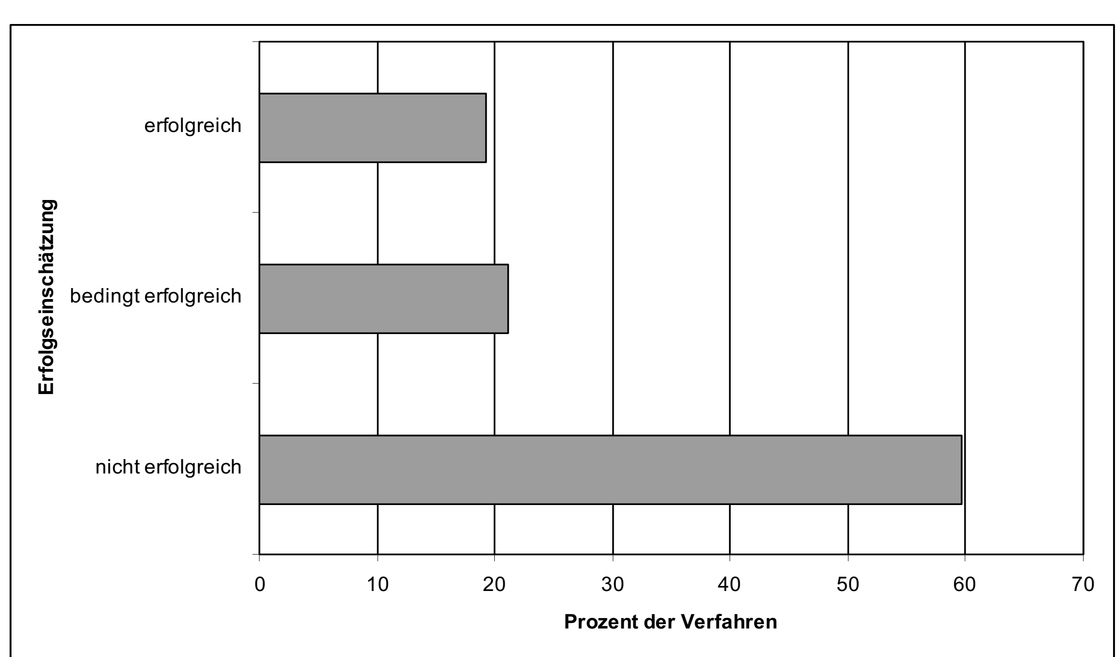
(1) Allgemeine Erfolgseinschätzung

In Bezug auf das Verfahren wird die Verkehrsdatenabfrage in den Akten und von den jeweiligen Bearbeitern in 19 Prozent als erfolgreich, in 21 Prozent als bedingt erfolgreich und in 60 Prozent als nicht erfolgreich eingestuft (Abbildung 116).

Die Einschätzung der Bearbeiter ist positiver als die in den Akten dokumentierten Hinweise. In den Akten wurden in 13 Prozent der Verfahren die Verkehrsdatenabfragen als erfolgreich und in 41 Prozent als nicht erfolgreich bezeichnet. Dagegen war nach Einschätzung der Bearbeiter die Ermittlungsmaßnahme in 6 Prozent der Verfahren erfolgreich, in 21 Prozent bedingt erfolgreich und in 19 Prozent nicht erfolgreich.

Abbildung 116

Erfolgseinschätzung für das Verfahren



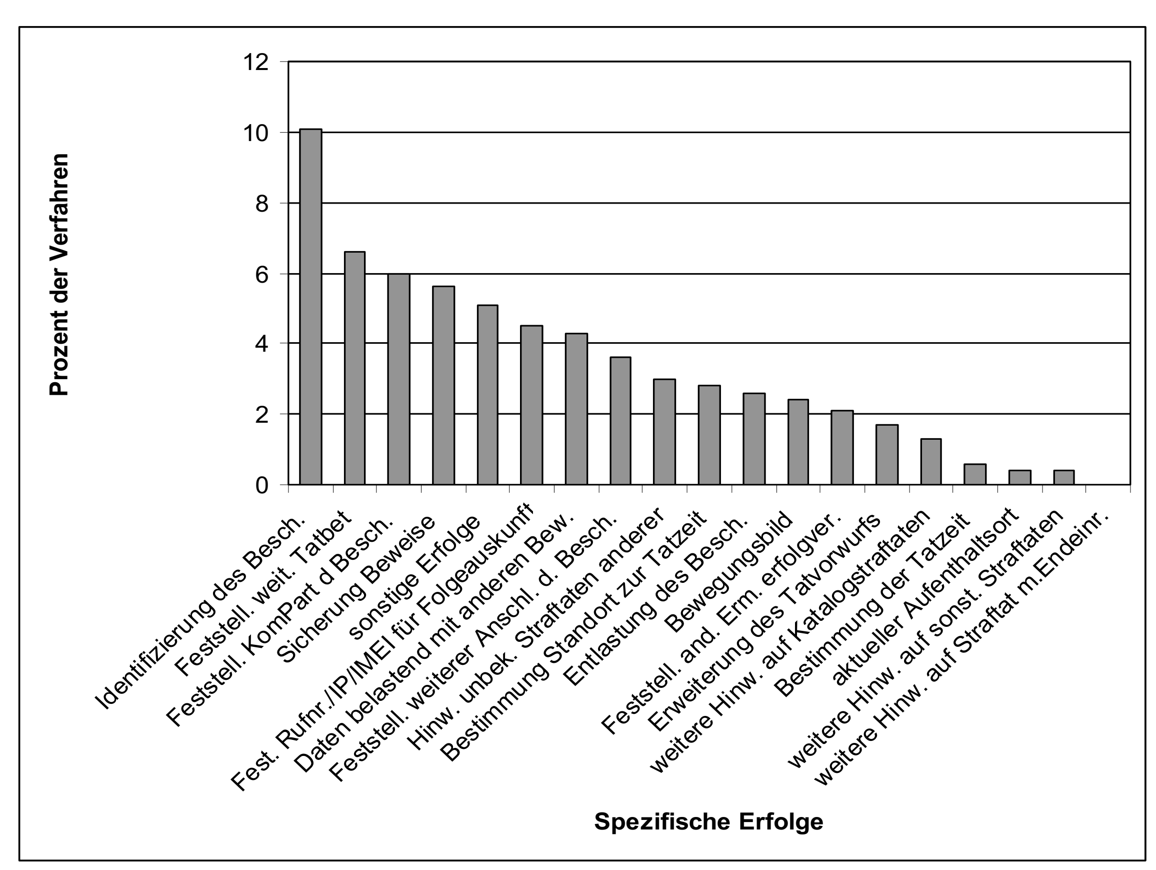
(2) Spezifische Erfolge in den Verfahren

Die spezifischen Erfolge, die sich aus den Verkehrsdatenabfragen für das jeweilige Verfahren ergeben haben, werden in Abbildung 117 dargestellt. Die Häufigkeit der konkreten Erfolge verteilt sich hier anders als bei den Beschlüssen. Der am häufigsten für das Verfahren festgestellte konkrete Erfolg ist die Identifizierung des Beschuldigten (10,1 Prozent der Verfahren). Ebenfalls häufig sind die Feststellung weiterer Tatbeteiligter (6,6 Prozent), die Feststellung von Kommunikationspartnern des Beschuldigten (6 Prozent) sowie die Sicherung von Beweisen (5,6 Prozent). Die belastende Wirkung der Verkehrsdaten mit anderen Beweismitteln (4,3 Prozent), die Feststellung von Rufnummern o. ä. für Folgeauskunftserteilungen (4,5 Prozent) sowie sonstige Erfolge (5,1 Prozent) sind etwas weniger häufig festgestellt worden. Ebenso in geringerem Maße konnten Erfolge wie die Feststellung weiterer Anschlüsse des Beschuldigten (3,6 Prozent), die Erlangung von Hinweisen auf unbekannte Straftaten anderer (3 Prozent), die Bestimmung des Standorts des Beschuldigten zur Tatzeit (2,8 Prozent) sowie die Entlastung des Beschuldigten (2,6 Prozent) und die Erstellung eines Bewegungsbildes (2,4 Prozent) mit der Verkehrsdatenabfrage erzielt werden. Die Feststellung, ob andere Ermittlungsmaßnahmen erfolgversprechend sein könnten, die Erweiterung des Tatvorwurfs, die Erlangung weiterer Hinweise auf Katalogstraftaten sowie die Bestimmung der Tatzeit konnte nur in geringem Umfang bewirkt werden. Die am seltensten erzielten Erfolge sind die Bestimmung des aktuellen Aufenthaltsorts des Beschuldigten und die Erlangung weiterer Hinweise auf sonstige Straftaten.

Bei zwei Drittel der Verfahren konnte kein spezifischer Erfolg der Verkehrsdatenabfrage festgestellt werden. Ansonsten variierte die Anzahl der genannten Erfolge pro Verfahren von einem bis zu 51. Dabei wurde am häufigsten ein Erfolg genannt (18 Prozent der Verfahren) und am zweithäufigsten zwei Erfolge pro Verfahren (7 Prozent). Zu jeweils 2 Prozent wurden drei und vier Erfolge in den Verfahren durch die Verkehrsdatenabfrage genannt. Fünf und zehn Erfolge wurden in jeweils 1 Prozent der Fälle erzielt.

Abbildung 117

Spezifische Erfolge im Verfahren



e) Beschuldigtenbezogene Erfolge

Bei 181 von 467 Verfahren (39 Prozent) konnte kein Täter identifiziert werden. In den restlichen 286 Verfahren gab es 697 Beschuldigte. Wie bereits ausgeführt konnten die Erfolge teilweise konkret auf die jeweiligen Beschuldigten bezogen werden. 367 Beschuldigten konnte kein beschuldigtenspezifischer Erfolg zugeordnet werden. Eine allgemein auf den Beschuldigten bezogene Einschätzung der Erfolge durch die Verkehrsdatenabfrage (aus der Akte oder durch den Bearbeiter) konnte bei 328 Beschuldigten abgegeben werden.

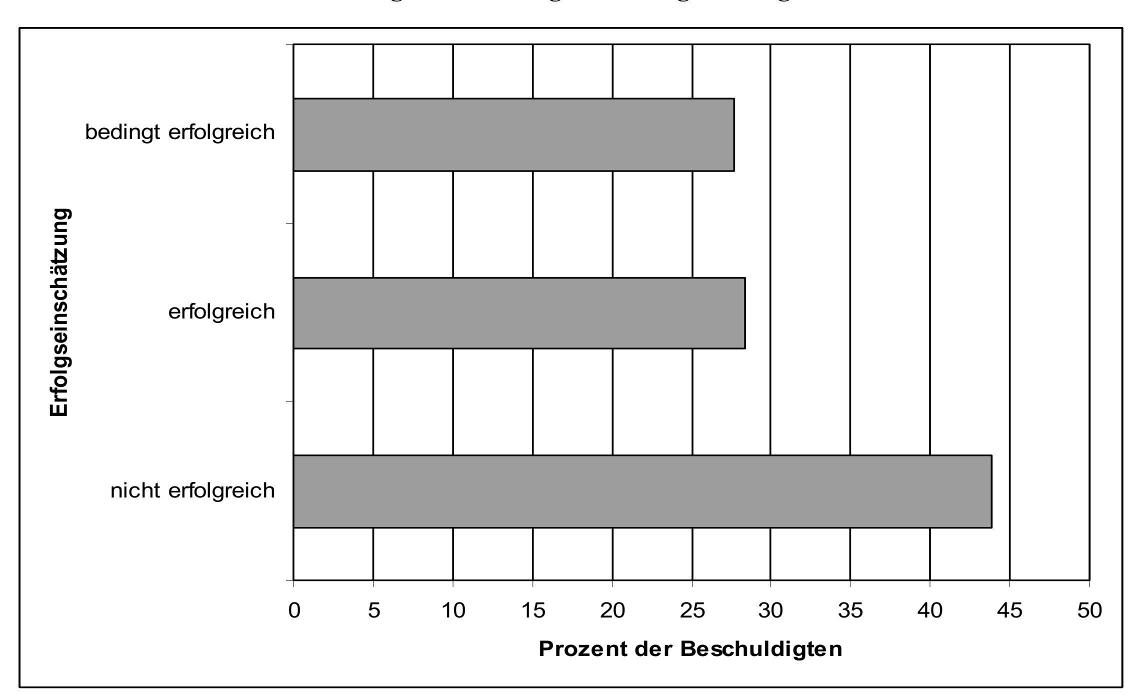
(1) Allgemeine Erfolgseinschätzung

Bei 35 Prozent der Beschuldigten konnte den Akten eine Erfolgseinschätzung entnommen werden. Bei 33 Prozent dieser Fälle wurde die Verkehrsdatenabfrage als erfolgreich eingeschätzt, bei 20 Prozent als bedingt erfolgreich und bei 47 Prozent als nicht erfolgreich. Zudem gaben die Bearbeiter ihre eigene Einschätzung ab. Bei 42 Prozent der Beschuldigten war eine solche Beurteilung möglich. Nach der Einschätzung der Bearbeiter war die Abfrage der Daten bei 26 Prozent der Beschuldigten erfolgreich, bei 31 Prozent bedingt erfolgreich und bei 43 Prozent nicht erfolgreich. In Abbildung 118 wird dargestellt, wie der Erfolg insgesamt, d. h. entweder aus der Akte oder nach eigener Einschätzung, beurteilt wird.

Dabei ist zu berücksichtigen, dass bei 369 Beschuldigten – das sind 53 Prozent der Beschuldigten – keine Erfolgeinschätzung abgegeben wurde. In diesen Fällen konnte der Erfolg nicht beschuldigtenbezogen beurteilt werden. Zusammengefasst wurde in den Akten und nach der Einschätzung der Bearbeiter bei 43,9 Prozent der Beschuldigten, bei denen eine Erfolgseinschätzung erfolgte, die Abfrage der Verkehrsdaten als nicht erfolgreich angesehen. Bei 27,7 Prozent der Beschuldigten wurde die Maßnahme als bedingt erfolgreich und bei 28,4 Prozent als erfolgreich eingeschätzt.

Abbildung 118

Erfolgseinschätzung beschuldigtenbezogen



(2) Spezifische Erfolge bezogen auf den Beschuldigten

Weiter konkretisiert werden konnten die Beurteilung des Erfolges bei 143 Beschuldigten (21 Prozent der Beschuldigten) Wie häufig welcher Erfolg in Bezug auf die Beschuldigten erzielt werden konnte, lässt sich Abbildung 119 entnehmen.

Genau wie bei den verfahrensbezogenen spezifischen Erfolgen ist auch in Bezug auf die Beschuldigten die Identifizierung des Beschuldigten der am häufigsten erzielte konkrete Erfolg (7 Prozent). Ebenfalls sehr häufig gelang die Feststellung von Kommunikationspartnern des Beschuldigten (5 Prozent), die Feststellung weiterer Tatbeteiligter (4,9 Prozent) sowie die Sicherung von Beweisen mit den Verkehrsdaten (4,4 Prozent). Bei 3,6 Prozent der Beschuldigten waren die Verkehrsdaten zusammen mit anderen Beweismitteln belastend für den Beschuldigten und bei 2,7 Prozent wurden weitere Anschlüsse des Beschuldigten festgestellt. Weniger häufig war die Bestimmung des Standorts des Beschuldigten zur Tatzeit (2,3 Prozent), die Erstellung eines Bewegungsbildes (2,2 Prozent), die Erlangung von Hinweisen auf unbekannte Straftaten anderer (2,2 Prozent), die Feststellung von Rufnummern für eine Folge-Auskunftserteilung (2 Prozent), die Erweiterung des Tatvorwurfs (1,7 Prozent), die Entlastung des Beschuldigten (1,7 Prozent) sowie die Feststellung, ob andere Ermittlungsmaßnahmen erfolgversprechend sein könnten (1,3 Prozent). Bei unter einem Prozent der Beschuldigten konnten weitere Hinweise auf Straftaten erlangt werden, konnte die Tatzeit sowie der aktuelle Aufenthaltsort des Beschuldigten festgestellt werden.

Wie bereits erwähnt konnten 143 Beschuldigten wenigstens ein spezifischer Erfolg zugeordnet werden. Dabei variierte die Anzahl der zuzuordnenden Erfolge von einem (77-mal, 54 Prozent) bis zu 51 (1-mal, 1 Prozent). Bei 22 Prozent dieser Beschuldigten wurden zwei Erfolge erzielt, bei 6 Prozent vier Erfolge, bei jeweils 4 Prozent drei, fünf und acht Erfolge, bei 2 Prozent sechs Erfolge und bei 1 Prozent sieben, neun, 17, 25 und 32 Erfolge.

Wenn man die Erfolgseinschätzungen für Verfahren, Beschuldigte und Beschluss gegenüberstellt, so fällt auf, dass die Verkehrsdatenabfrage auf den Beschuldigten bezogen erfolgreicher ist (Abbildung 120). Allerdings ist dabei zu berücksichtigen, dass bei 53 Prozent der Beschuldigten keine Erfolgseinschätzung speziell für den Beschuldigten möglich war.

Abbildung 119



Spezifische Erfolge bezogen auf die Beschuldigten

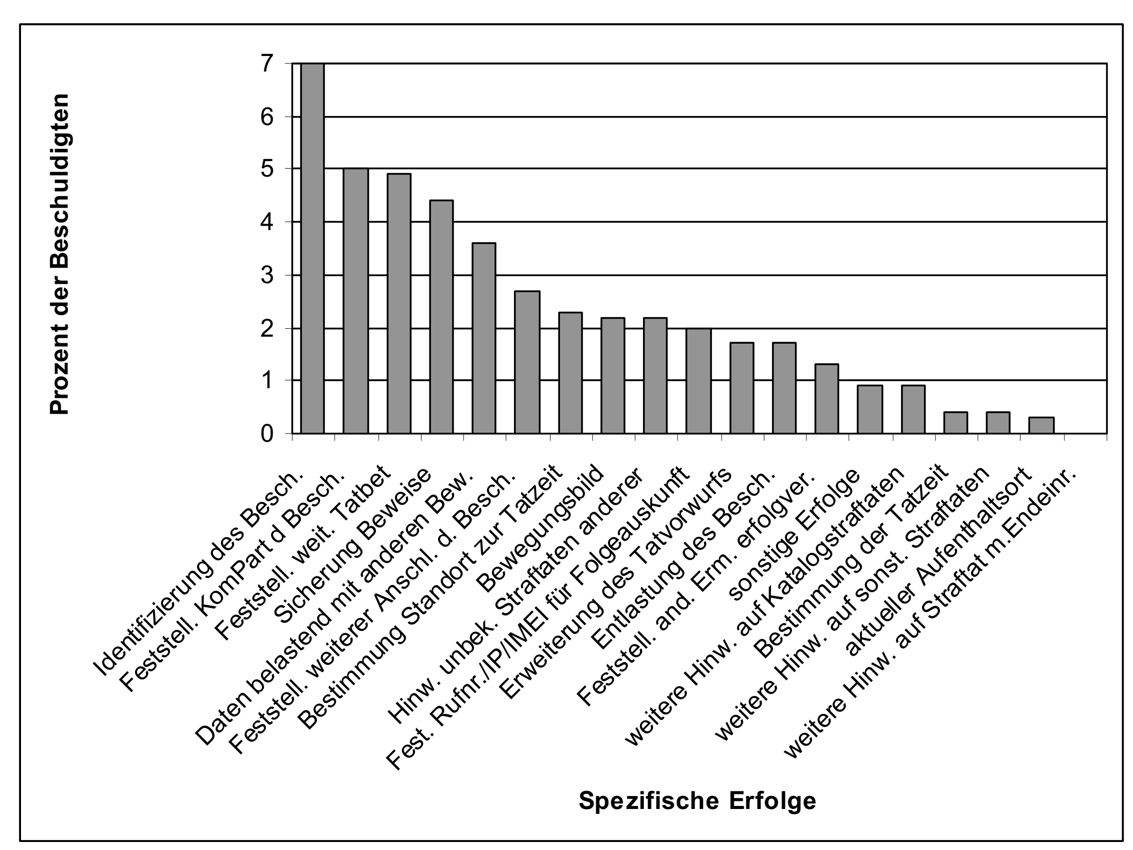
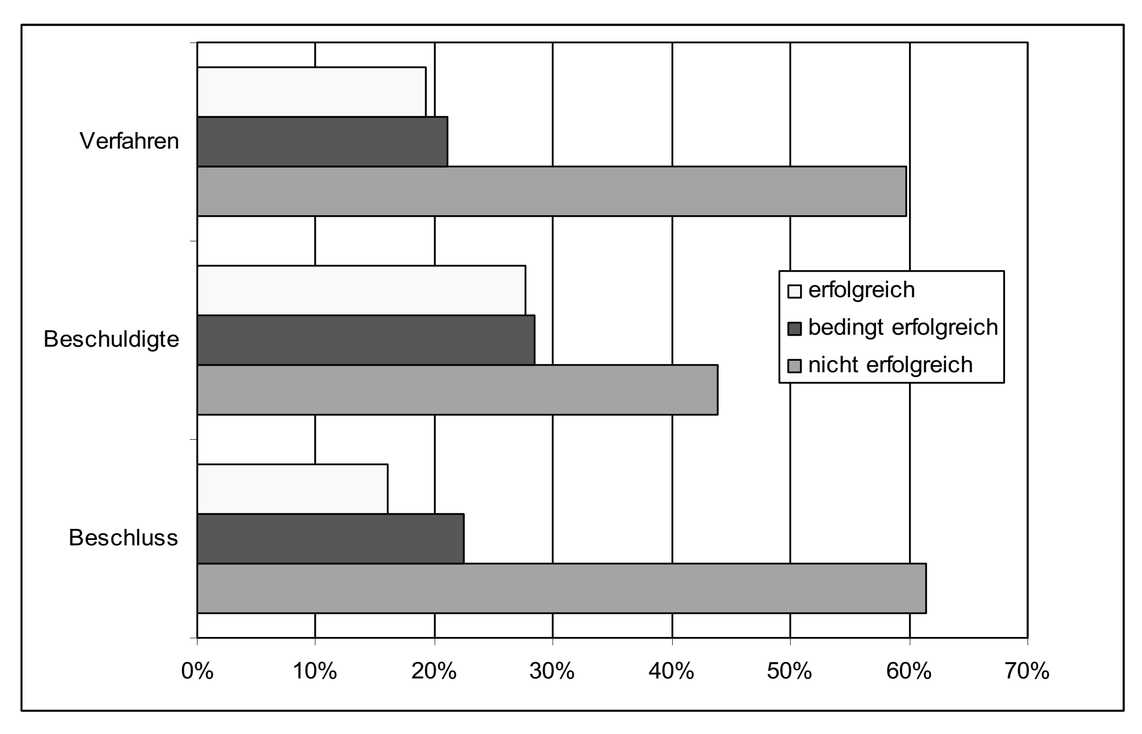


Abbildung 120

Vergleich der Erfolgseinschätzungen



f) Differenzierung der Erfolge nach Delikten

Tabelle 27 zeigt, wie erfolgreich die Verkehrsdatenabfragen differenziert nach Katalogdelikten, die mit den Maßnahmen aufgeklärt werden sollten, waren. In Bezug auf den Mittelwert bedeutet eins „erfolgreich“, zwei „bedingt erfolgreich“ und drei „nicht erfolgreich“. Am erfolgreichsten war die Abfrage der Verkehrsdaten nach den Ergebnissen der Aktenauswertung bei den Straftaten gegen die persönliche Freiheit, bei Geld- und Wertpapierfälschungen sowie bei Erpressungen. Hier waren die Beschlüsse erfolgreich bis bedingt erfolgreich. Die geringsten Erfolge waren bei Ausländerstraftaten und Tötungsdelikten zu verzeichnen. Die Ergebnisse zum Erfolg bei Friedensverrat, schwerer sexueller Missbrauch von Kindern sowie Verstöße gegen das Waffengesetz sind wegen der geringen Anzahl von Fällen nicht aussagekräftig.

In Tabelle 28 werden die Erfolge der sonstigen Delikte, die nicht unter den Straftatenkatalog des § 100a Satz 1 StPO fallen, dargestellt.

Tabelle 27

Erfolge differenziert nach Katalogdelikten

	erfolgreich (1)	**bedingt erfolgreich**	**nicht erfolgreich (3)**	**insg.**	**Mittel**
Friedensverrat etc.	0	0	1	1	3,0
öff. Ordnung	2	0	3	5	2,2
Geld-/Wertp.Fälsch	2	1	1	4	1,8
schw.sex.Missbr.Kinder	0	0	1	1	3,0
Mord/Totschlag	12	22	79	113	2,6
ST.gg.pers.Freiheit	5	2	2	9	1,7

noch Tabelle 27

Erfolge differenziert nach Katalogdelikten

	erfolgreich (1)	**bedingt erfolgreich**	**nicht erfolgreich (3)**	**insg.**	**Mittel**
(schw)Band.Diebst.	10	7	31	48	2,4
Raub/räub.Erpr.	25	47	84	156	2,4
Erpressung	4	2	3	9	1,9
gew.Hehl./BandHehl.	0	10	1	11	2,1
Geldwäsche etc	0	9	3	12	2,3
gemein gef StrfT	1	0	4	5	2,6
WaffG/AußenwG/KrKG	0	0	2	2	3,0
BtMG	21	21	77	119	2,5
AuslG/AufG/AsylVfG	6	4	34	44	2,6
Insg.	**77**	**110**	**288**	**475**	**2,44**

Tabelle 28

Erfolge differenziert nach sonstigen Delikten

	erfolgreich (1)	**bedingt erfolgreich**	**nicht erfolgreich (3)**	**insg.**	**Mittel**
einfacher Diebstahl	3	3	11	17	2,47
sonstiges	5	8	12	25	2,28
ST.gg.sex.Selbstbest	4	0	7	11	2,27
ST.gg.pers.Freih.	5	4	14	23	2,39
schw. Diebst.	8	23	58	89	2,56
Hehlerei	0	0	1	1	3,00
gemeingef.ST	0	1	1	2	2,50
BtMG (nicht § 100a)	0	1	2	3	2,67
AuslR (nicht § 100a)	0	0	3	3	3,00
Betrug	8	8	53	69	2,65
KörpVerlDel	0	1	6	7	2,86
Androh.ST	3	3	7	13	2,31
Beleidigung	7	5	11	23	2,17
SpezCompKrim	0	1	0	1	2,00
Mißbr.Notruf	3	0	0	3	1,00
Insg.	**43**	**56**	**173**	**272**	**2,48**

Am erfolgreichsten war die Verkehrsdatenabfrage bei der Aufklärung von Beleidigungsdelikten. Bei diesen handelt es sich um mittels Endeinrichtung begangene Straftaten, die teilweise nur mit der Abfrage der Verkehrsdaten aufgeklärt werden können. Relativ erfolglos blieb die Abfrage der Daten bei Körperverletzungsdelikten und bei Betrugsstraftaten.

g) Erfolge differenziert nach der Art der Verkehrsdatenabfrage

In Bezug auf die Art der Verkehrsdatenabfrage gestaltet sich die Erfolgsquote wie in Abbildung 121 und Tabelle 29 dargestellt.

Abbildung 121



Erfolge differenziert nach der Art der Abfrage

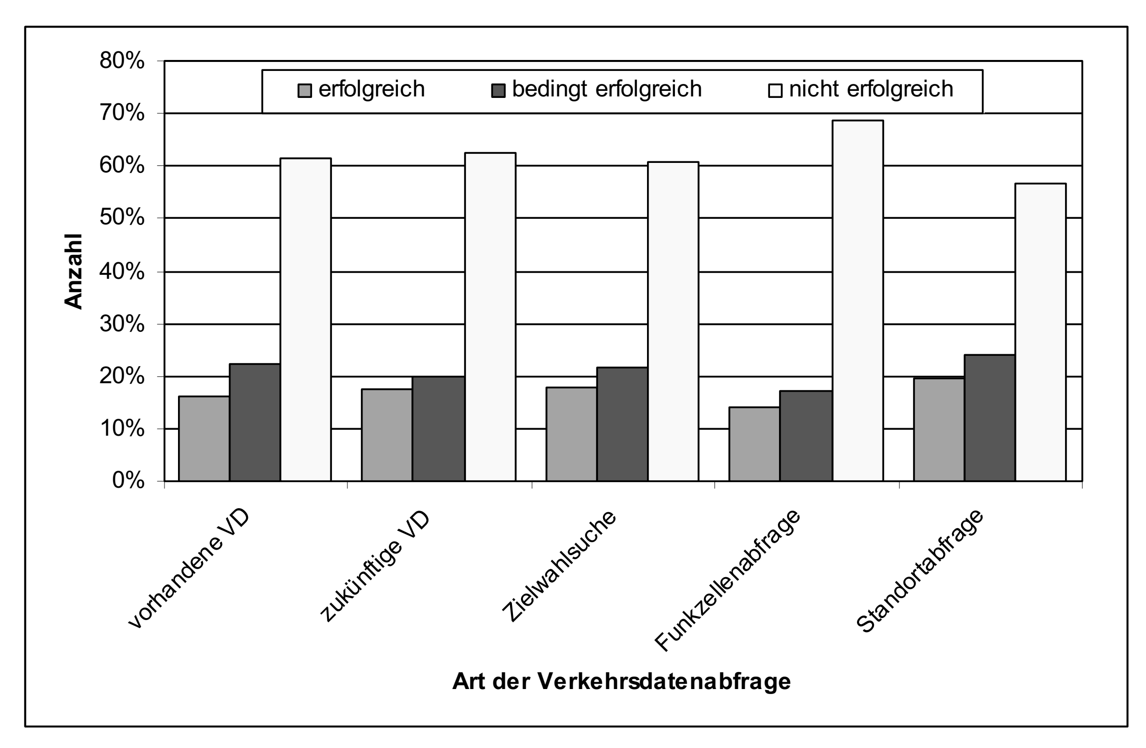


Tabelle 29

Erfolge der einzelnen Abfragearten

	Erfolgreich (1)	bedingt erfolgreich	nicht erfolgreich (3)	insg.	Mittel
vorhandene VD	110	151	418	679	2,45
zukünftige VD	46	53	166	265	2,45
Zielwahlsuche	75	91	258	424	2,43
Funkzellenabfrage	9	11	44	64	2,55
Standortabfrage	26	32	76	134	2,37
sonstiges	5	9	7	21	2,10
insg.	**116**	**165**	**446**	**727**	**2,45**

Am erfolgreichsten mag noch die Standortabfrage sein, während die Funkzellenabfrage die geringsten Erfolge aufweist. Es sind aber keine signifikanten Unterschiede festzustellen.

3. Experteninterviews

a) Polizeibeamte

(1) Ermittlungserfolge

Von den befragten Polizeibeamten wurden mehrere Ermittlungserfolge, die sich mit der Verkehrsdatenabfrage erzielen lassen, genannt. Zum einen könne man Strukturen ermitteln, Kontakte nachweisen und Tatbeteiligungen feststellen. Es sei wichtig herauszufinden, in welchem Umfeld sich die Täter bewegen, Gruppen festzustellen und Verbindungen zu erkennen oder zu bestimmen, wer nur „zufällig“ in die Ermittlungen hineingeraten sei. Es lasse sich dann das Ausmaß von Treffen und Kontakten feststellen. Die Maßnahme sei zur Täteridentifizierung und zur Aufklärung der Straftat bedeutsam. Der identifizierte Anschlussinhaber müsse aber nicht immer der Täter sein.

Zudem sei die Anwesenheit zu einem bestimmten Zeitpunkt an einem bestimmten Ort zu bestimmen. Es könne nachgewiesen werden, dass sich ein bestimmtes Mobiltelefon am Tatort oder in Tatortnähe befunden habe. Die Verkehrsdatenabfrage sei ein wichtiges Ermittlungsinstrument zur Standortbestimmung. Ein anderer Befragter gibt an, dass es sich dabei aber nur um Indizien handle und nicht um Beweise. Man könne nur den Aufenthaltsort eines Mobiltelefons, nicht den einer Person bestimmen. Zur Vorbereitung von Telekommunikationsüberwachungsmaßnahmen könne man Anschlüsse des Beschuldigten feststellen, um gezielt die Überwachung zu beginnen. §§ 100g, 100h-Maßnahmen würden insoweit häufig mit §§ 100a, 100b-Maßnahmen kombiniert.

Es gehe darum, aus einem Anfangsverdacht einen konkreten Verdacht zu machen. Das Erhärten und Verifizieren eines Tatverdachts sei möglich. Verkehrsdaten böten danach einen Ermittlungsansatz, um einen vorhandenen Verdacht zu verdichten. Bereits vorhandene Erkenntnisse könnten damit untermauert werden. Zudem könne die Verkehrsdatenabfrage überhaupt erst zur Gewinnung eines Anfangsverdachts gegen eine konkrete Person führen. Die Daten könnten zu vielfältigen Zwecken ausgewertet werden. Es gebe Anhaltspunkte für weitere Ermittlungen in dem Sinne, ob es sich lohne, in eine Richtung weiterzuermitteln. Die Ermittlungen würden dadurch in die richtige Richtung gelenkt. Funkzellenabfragen seien gerade bei Raubfällen und Tötungsdelikten sinnvoll. Bei mehreren Tätern werde oft vor, während und nach der Tat telefoniert. Die Daten würden dem Beschuldigten zudem in der Vernehmung vorgehalten, um den Druck zu einem Geständnis zu verstärken.

(2) Dezernatsspezifische Bedeutung

Die Frage, welche Bedeutung die Maßnahme nach §§ 100g, 100h StPO speziell in ihrem Dezernat einnehme, beantworteten die Befragten unterschiedlich. Die Polizeibeamten aus Betäubungsmittel- und organisierte Kriminalität-Abteilungen gaben zumeist an, dass die Verkehrsdatenabfrage eine hohe Bedeutung in ihrem Dezernat einnehme. Oft sei die Maßnahme das einzige Mittel, um den Beschuldigten zu ermitteln, und diene ferner zur Vorbereitung anderer verdeckter Ermittlungsmaßnahmen (wie Telefonüberwachung, Observation). Von zwei der Befragten aus diesen Bereichen wurde die Maßnahme als unverzichtbar bezeichnet. Ein Befragter aus dem Betäubungsmittelbereich gab an, dass die Bedeutung fallbezogen sei. Es sei ein Mittel, das regelmäßig benutzt werde, trete aber hinter den §§ 100a, 163f StPO weit zurück. Auch ein Befragter aus dem organisierte Kriminalität-Bereich bezeichnet §§ 100a, 100b als wesentlich wichtiger, aber die Verkehrsdaten würden häufig einen Ermittlungsansatz liefern, der zur Bestärkung eines Verdachts führe. Bei den Befragten aus den Abteilungen mit Raubdelikten, Bandenkriminalität, Erpressung und Entführung wurde von alle Befragten eine hohe Bedeutung der Verkehrsdatenabfrage angegeben. Die Täter würden bei Überfällen auf Geschäfte/Banken/Geldtransporter häufig ein Mobiltelefon für Absprachen während der Tat nutzen. Gerade bei unbekannten Tätern, die Raubdelikte begangen hätten, könnte anhand der Funkzellenabfrage festgestellt werden, wer zur Tatzeit am Tatort gewesen sei. Die Maßnahme nehme daher einen sehr hohen Stellenwert ein. Auch ein Befragter aus der Abteilung Todesermittlungen und Sexualdelikte verweist auf die große Bedeutung. Ein Befragter aus der Abteilung Finanzermittlungen/Geldwäsche räumt der Verkehrsdatenabfrage dagegen nur eine untergeordnete Rolle ein. Die Maßnahme habe in diesem Feld keine besondere Bedeutung. Bei Wirtschaftskriminalität sei die Durchführung eher die Ausnahme, obwohl die Voraussetzungen oft gegeben seien. Die meisten Befragten aus der Telekommunikationsüberwachungsüberwachungs- bzw. Computerabteilung sind demgegenüber der Meinung, dass die Maßnahme eine erhebliche Bedeutung habe. Oft kennzeichne sie den entscheidenden Punkt in den Ermittlungen. Ein weiterer Befragter aus einer Telekommunikationsüberwachungsabteilung gibt an, dass die §§ 100gh-Maßnahmen von der Masse her stark ausgeprägt seien, von der Wertigkeit würden sie hinter § 100a StPO freilich nur den zweiten Rang einnehmen.

b) Staatsanwälte

(1) Ermittlungserfolge

Ermittlungserfolge der Verkehrsdatenabfrage betreffen aus der Sicht der Staatsanwälte vor allem die Identifizierung der Beschuldigten bzw. des Täters sowie die Standortfeststellung, mit der Tatortnachweise geführt werden könnten. Die Erstellung von Bewegungsbildern sei möglich. Anhand der Positionsdaten könnten Personen identifiziert und Taten zugeordnet werden. So werde eine „Tatablaufermittlung“ möglich. Zudem könnten Verbindungen zu anderen Bandenmitgliedern nachgewiesen werden. Es ließen sich Kontakte, Betäubungsmittel-Schienen, Netzverzweigungen und Beziehungsgeflechte feststellen. Die Maßnahme liefere wertvolle Ermittlungsansätze für weitere Ermittlungen. Auch Vorhalte würden

möglich. Teilweise wurde vor allem die Zielwahlsuche als erfolgversprechend hervorgehoben.

Weiter wurde angegeben, dass die Frage des Erfolgs straftat- bzw. einzelfallabhängig sei und nicht zu pauschalisiert betrachtet werden dürfe. Manche Straftaten könnten nur mit einer Funkzellenabfrage aufgeklärt werden. Der Normalfall sei, dass weitergehende Ermittlungsansätze damit erlangt werden könnten (z. B. wenn die IP-Adresse ermittelt werde, könne dann über diese weiterermittelt werden). Früher habe es einen Überraschungseffekt gegeben, meint ein Befragter. Deshalb sei die Maßnahme am Anfang sehr erfolgreich gewesen. Mittlerweile würden sich professionelle Täter aber darauf einstellen und aus dem Ausland heraus arbeiten. Ein Befragter meint, dass die Erfolge ebenso wie bei der Telefonüberwachung immer mittelbar seien. Die Nummer werde festgestellt, das sage aber nichts über die Täterschaft aus. Ein weiterer Befragter gibt an, dass die Abfrage nur ein Hilfsmittel sei. Die Verkehrsdaten lieferten Indizien für Beziehungen von Personen untereinander sowie dafür, dass Auslandsfahrten stattgefunden hätten. Aber wer sich dahinter als konkreter Täter verberge, könne damit nicht nachgewiesen werden. Eine Überführung sei auch deshalb schwer, da beim Kauf von Telefonkarten die Personalien nicht überprüft werden würden.

(2) Dezernatsspezifische Bedeutung

Die dezernatsspezifische Bedeutung wird auch von den befragten Staatsanwälten unterschiedlich beurteilt. Im organisierte Kriminalität- und Betäubungsmittel-Bereich wird die Bedeutung teilweise als relativ hoch eingeschätzt. Sie gehöre zum Standardrepertoire. Man könne Bezüge der Täter untereinander herstellen und wichtige Hinweise auf Strukturen der Täter erlangen. Diejenigen, die der Maßnahme im organisierte Kriminalität- und Betäubungsmittel-Bereich eine geringe Bedeutung zuordnen, überwiegen jedoch leicht. Die Maßnahme komme nur in Fällen zum Einsatz, in denen keine weiteren Ermittlungsansätze vorlägen und der Täter noch unbekannt sei, und sei daher eher die Ausnahme. Die Maßnahme sei von eher untergeordneter Bedeutung bzw. die Bedeutung sei relativ gering. Ein Befragter führt aus, dass die Maßnahme selten vorkomme, aber wenn sie durchgeführt würde, könnten gute Erfolge damit erzielt werden. Im Bereich der Computerkriminalität wird der Verkehrsdatenabfrage eine besonders hohe Bedeutung zugewiesen. Sie sei in diesem Bereich unverzichtbar. Die Daten könnten teilweise auch durch ein einfaches Auskunftsersuchen erfragt werden, so dass nicht in allen Fällen ein Beschluss beantragt werden müsse. Dennoch sei die Bedeutung wesentlich. Die Bedeutung der Maßnahme nehme auch bei allgemeiner Kriminalität zu. Dort habe sie aber eine geringere Bedeutung als eine Durchsuchung. Im Wirtschaftskriminalitätsbereich ist die Maßnahme nach Ansicht der Befragten von eher untergeordneter Bedeutung.

c) Richter

Ermittlungserfolge, die mit der Verkehrsdatenabfrage zu bewirken sind, sei u. a. die Feststellung, ob der Täter am Tatort war. Die Standortfeststellung sei relativ erfolgreich. Daneben sei die Informationssammlung von hoher Bedeutung, auch was Standortdaten angehe. Die Daten würden zur Überführung bzw. zur Identifizierung des Täters beitragen. Es könnten aber auch entlastende Informationen in Erfahrung gebracht werden. Vor allem bei Drogenkriminalität könnten Lieferanten und Verkäufer häufig über die Verkehrsdatenabfrage identifiziert werden. Es könnten Kontakte geklärt werden, aber durch §§ 100g, 100h StPO könnten keine Inhalte ermittelt werden. Außerdem fände ein regelmäßiger Austausch der SIM-Karte statt. Der Fall, dass mit einem gestohlenen Mobiltelefon weiter telefoniert und nicht die Karte ausgetauscht oder das Telefon verkauft werde, sei selten. Ein Befragter schätzt die Funkzellenabfrage als eine „Suche nach der Nadel im Heuhaufen“ ein.

d) Verteidiger

Ein Verteidiger berichtete von einer Verfahrenskonstellation, in der durch Verkehrsdaten ein Alibibeweis hätte geführt werden können. Ansonsten wurden keine Fälle geschildert, in denen eine Auskunftserteilung für den Mandanten Erfolg versprechend gewesen wäre.

4. Zusammenfassung der Ergebnisse

Den Akten konnte entnommen werden, dass die Verkehrsdatenabfrage im Ermittlungsverfahren bedingt erfolgreich ist. Bezogen auf die Anschlüsse überwiegen eindeutig die Fälle, bei denen die Abfrage der Daten als nicht erfolgreich eingeschätzt wurden, und auch die Beschlüsse wurden zu zwei Dritteln als nicht erfolgreich eingestuft (in der Akte oder von den jeweiligen Bearbeitern). In Bezug auf das Verfahren erscheint die Verkehrsdatenabfrage zu 19 Prozent als erfolgreich, zu 21 Prozent als bedingt erfolgreich und zu 60 Prozent als nicht erfolgreich. Auf den Beschuldigten bezogen kann die Abfrage der Daten bei 27,7 Prozent als bedingt erfolgreich, bei 28,4 Prozent als erfolgreich und bei 43,9 Prozent als nicht erfolgreich eingestuft werden.

Spezifische Erfolge, die bei den Beschlüssen erreicht werden konnten, waren vor allem die Feststellung weiterer Tatbeteiligter sowie die Identifizierung des noch unbekannten Beschuldigten. Aber auch die Feststellung von Kommunikationspartnern und die Sicherung von Beweisen konnten mit der Abfrage der Daten häufig erreicht werden. Pro Beschluss konnten bis zu 32 Erfolge erzielt werden. Das sind jedoch Ausnahmefälle. Am häufigsten wurde ein einzelner spezifischer Erfolg erreicht. Wird das mit den Beschlüssen verfolgte Ziel zum Ausgangspunkt genommen, dann fällt auf, dass dieses häufig nicht erreicht, aber dafür andere Erfolge erzielt wurden. Das häufigste in den Akten dokumentierte Ziel war die Identifizierung des noch unbekannten Täters. Die Identifizierung erfolgte jedoch nur in 8 Prozent der Fälle. Ein eher seltenes Ziel, aber häufig erreichter Erfolg, war beispielsweise die Bestimmung des Standortes des Beschuldigten bzw. des Mobiltelefons zur Tatzeit. Zu berücksichtigen ist hierbei, dass – was sich auch aus den Expertengesprächen ergibt – die Verkehrsdatenabfrage häufig der erste Ansatz-

punkt für Ermittlungen ist. Es ist deshalb möglich, dass die Identifizierung des unbekannten Täters oder die Aufklärung des Sachverhalts eher allgemein in den Beschlüssen genannt wurden, gerade weil noch keine anderen Ermittlungsansätze vorliegen. Von den verfahrens- und beschuldigtenspezifischen konkreten Erfolgen unterscheiden sich die beschlussbezogenen Erfolge kaum. Allerdings ist bei diesen die Identifizierung des Beschuldigten der am häufigsten erzielte Erfolg.

Ermittlungserfolge, die von den interviewten Experten angegeben wurden, betrafen die Ermittlung von Strukturen und Kontakten zwischen Tatbeteiligten sowie die Identifizierung des Täters. Ferner wurden die Bestimmung des Standorts des Beschuldigten zur Tatzeit sowie die Erstellung von Bewegungsbildern genannt. Allerdings wird in diesem Zusammenhang auf die Indizfunktion der Daten hingewiesen. Die Daten können nur Anhaltspunkte dafür geben, wo sich das Mobiltelefon befunden hat. Zur Vorbereitung von Telekommunikationsüberwachungen werden mit der Verkehrsdatenabfrage Anschlüsse festgestellt. Die Daten führen teilweise erst zur Gewinnung eines Anfangsverdachts gegen eine bestimmte Person und sollen zu Anhaltspunkten für weitere Ermittlungsmaßnahmen führen. Daneben wird den Daten auch eine gewisse Bedeutung im Versuch zugewiesen, den Beschuldigten zu einem Geständnis zu bewegen. Gerade im organisierte Kriminalität- und Betäubungsmittel-Bereich sowie bei Raubdelikten, Bandenkriminalität und Computerkriminalität hat die Verkehrsdatenabfrage nach Angabe der meisten Befragten eine große Bedeutung. Von den schriftlich Befragten geben 63 Prozent an, dass die Maßnahmen unverzichtbar seien.

IV. Erfolge der Verkehrsdatenabfrage im weiteren Verfahrensverlauf

1. Schriftliche Befragung

Anhand der schriftlichen Befragung wurde die Effizienz der Verkehrsdatenabfrage über das Ermittlungsverfahren hinaus nicht explizit erfasst. Die Ergebnisse der schriftlichen Befragung zur Effizienz der Maßnahme allgemein sind jedoch bei den Erfolgen im Rahmen des Ermittlungsverfahrens sowie im Rahmen des Verhältnisses zur Telekommunikationsüberwachung und zu anderen Ermittlungsmaßnahmen aufgeführt.

2. Aktenanalyse

a) Zusammenhang zwischen Verfahrensausgang und Erfolg der Verkehrsdatenabfrage

Ein weiterer Indikator für die Effizienz der Verkehrsdatenabfrage liegt im Ausgang des Verfahrens. Wie die Verfahren abgeschlossen wurden, wurde bereits im Abschnitt über den Verfahrensausgang erörtert. In knapp 60 Prozent der Fälle wurde das Verfahren eingestellt. Anklage (mit Strafbefehlsanträgen) wurde in 23 Prozent der Fälle erhoben. In 18 Prozent der Fälle war das Verfahren noch nicht abgeschlossen oder es war aus anderen Gründen nicht möglich, den Verfahrensausgang zu ermitteln. Wenn Anklage erhoben wurde, wurden die Angeklagten in 85 Prozent der Fälle verurteilt. Teileinstellung und Teilfreispruch erfolgten zu jeweils 1 Prozent. Freigesprochen wurden die Beschuldigten in 6 Prozent der Fälle und in 7 Prozent der Fälle wurde das Verfahren gegen die Angeklagten durch das Gericht eingestellt.

Zur Beurteilung der Effizienz kann nunmehr überprüft werden, wie das Verfahren abgeschlossen wurde, wenn die Verkehrsdatenabfrage erfolgreich bzw. nicht erfolgreich war. Abbildung 122 zeigt, dass in den Fällen, in denen die Verkehrsdatenabfrage in den Akten oder von den Bearbeitern der Akte als erfolgreich eingestuft wurde, die Anklagequote im Vergleich zu den anderen Fallgruppen deutlich erhöht ist. Dementsprechend nimmt die Einstellungsquote mit der Erfolglosigkeit der Verkehrsdatenabfrage drastisch zu. Freilich handelt es sich damit um einen Indikator, mit dem eine Kausalität zwischen Verkehrsdatenabfrage und der Entscheidung über Anklage und Einstellung nicht hergestellt werden kann.

In Abbildung 123 werden Zusammenhänge zwischen dem Erfolg der Verkehrsdatenabfrage und dem Ausgang der Hauptverhandlung vorgestellt. Die Verurteilungsrate ist dann besonders ausgeprägt, wenn die Verkehrsdatenabfrage erfolgreich war. Freilich ist die Verurteilungsquote auch in den anderen Fallgruppen hoch. Insoweit macht sich eine spezifische Selektion durch die Anklageentscheidung bemerkbar, die insgesamt dazu führt, dass im Wesentlichen erfolgversprechende Fälle einer Anklage zugeführt werden.

b) Beweismittel in der Anklageschrift

Die 286 Verfahren gegen bekannte Beschuldigte betrafen 697 Beschuldigte. Gegen insgesamt 211 Beschuldigte wurde Anklage[468] (28 Prozent) erhoben oder Strafbefehl (2 Prozent) beantragt. Gegen 333 identifizierte Beschuldigte (48 Prozent) wurde das Verfahren eingestellt. Bei weiteren 153 Beschuldigten (22 Prozent) konnte den Akten kein Verfahrensausgang entnommen werden. Bei 91 Prozent der Beschuldigten wurde mindestens eines der unten genannten Beweismittel in der Anklageschrift erwähnt. In 11 Prozent der Anklageschriften wurde ein Beweismittel aufgeführt, in 30 Prozent zwei Beweismittel und in 37 Prozent drei Beweismittel. Vier Beweismittel wurden in 16 Prozent der Anklagen genannt und fünf Beweismittel in 7 Prozent. Als Beweismittel spielten die Verkehrsdaten in den überprüften Verfahren zahlenmäßig eine eher untergeordnete Bedeutung. Bei 13 Prozent der Beschuldigten wurden die Verkehrsdaten in der Anklage als Beweismittel aufgeführt. Wie sich die Häufigkeit der Beweismittel auf die Anklageschriften verteilt hat, kann Abbildung 124 entnommen werden. Am häufigsten wurden Zeugenaussagen (90 Prozent der Anklageschriften) als Beweismittel in den Anklageschriften verwendet. Als Beweismittel bedeutsam waren zudem Augenscheinsobjekte wie beschlagnahmte Mobiltelefone und die in Ver-

[468] Auch Teileinstellungen wurden an dieser Stelle unter die Anklage subsumiert.

Abbildung 122

Verhältnis von Anklage und Einstellung zum Erfolg der Verkehrsdatenabfrage

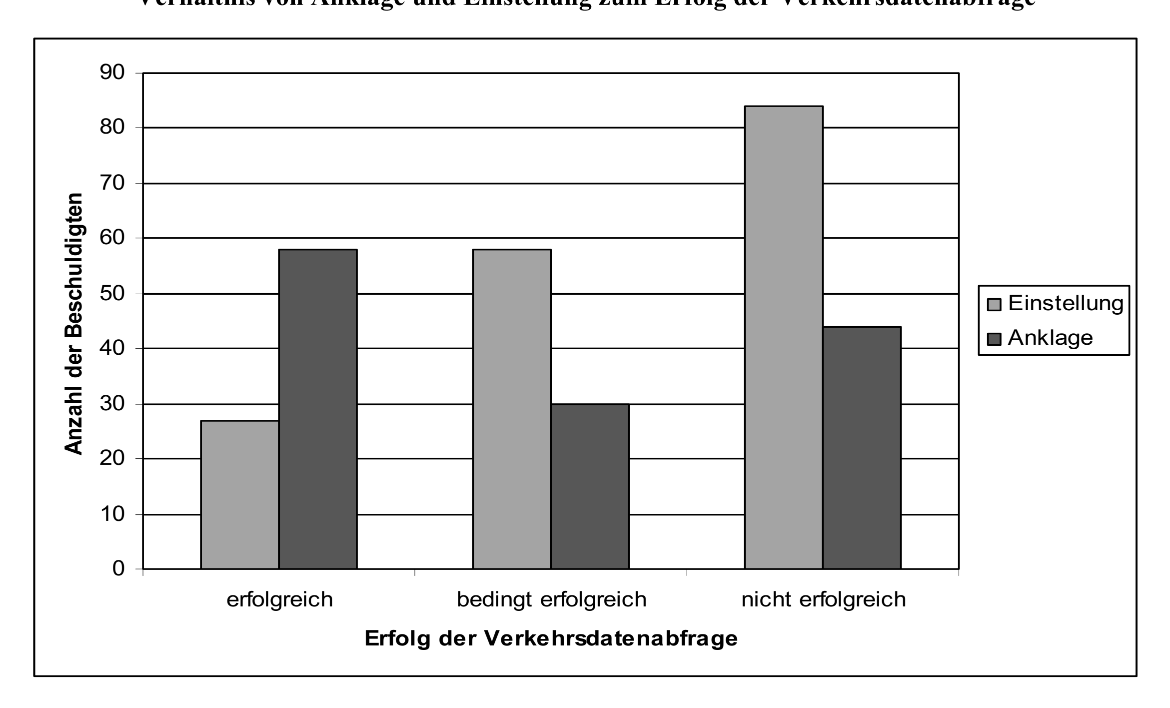
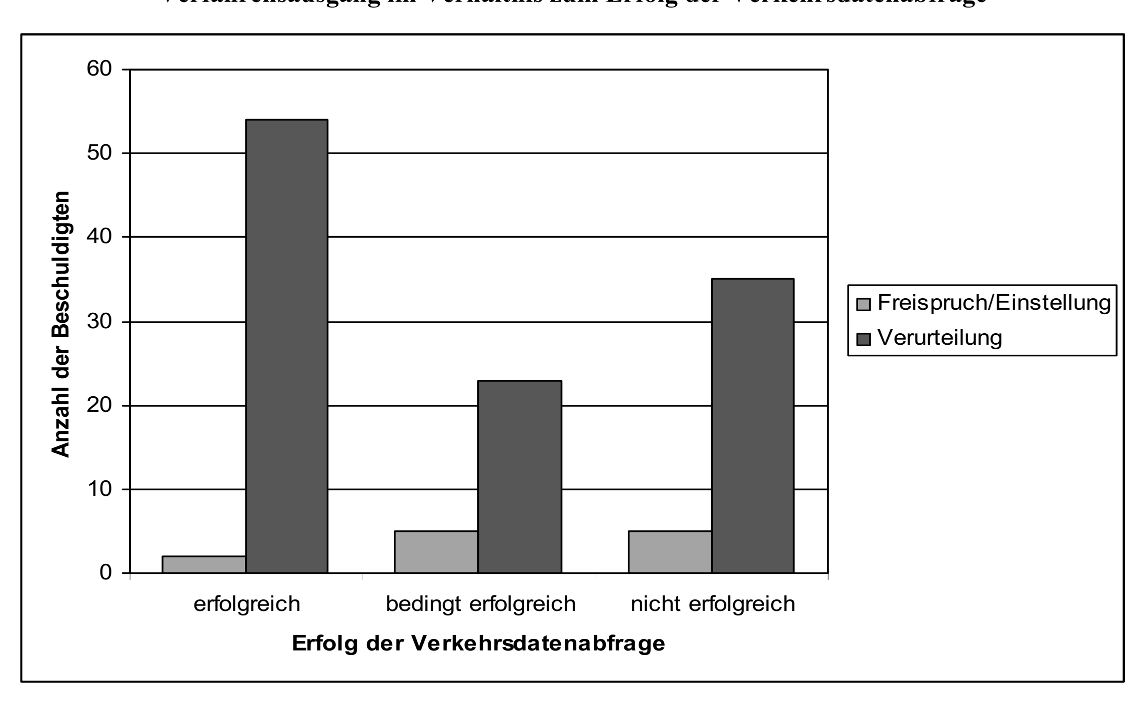


Abbildung 123

Verfahrensausgang im Verhältnis zum Erfolg der Verkehrsdatenabfrage



fahren wegen Betäubungsmittelstraftaten beschlagnahmten Drogen (48 Prozent). Relativ häufig waren zudem die Einlassung der Beschuldigten (32 Prozent) sowie Telefonüberwachungsprotokolle (30 Prozent). Urkunden (22 Prozent) und Geständnisse (19 Prozent) dienen ebenfalls als Beweismittel. Sachverständigengutachten (10 Prozent), Durchsuchungsprotokolle (9 Prozent), Observationsprotokolle (4 Prozent) und Anschlussinhaberfeststellungen (3 Prozent) wurden in den Anklagen weniger häufig genannt. Bei 9 Prozent der angeklagten Beschuldigten konnte den Akten nicht entnommen werden, welche Beweismittel in der Anklage aufgeführt wurden. Das war dann der Fall, wenn die Anklageschrift in den Akten fehlte, aber ersichtlich war, dass Anklage erhoben wurde.

In der Häufigkeit der Nennungen einzelner Beweismittel können keine Unterschiede hinsichtlich Teileinstellung, Anklage oder Strafbefehl festgestellt werden, was allerdings angesichts der geringen Anzahl von Teileinstellungen (9) und Strafbefehlen (15) auch nicht zu erwarten war.

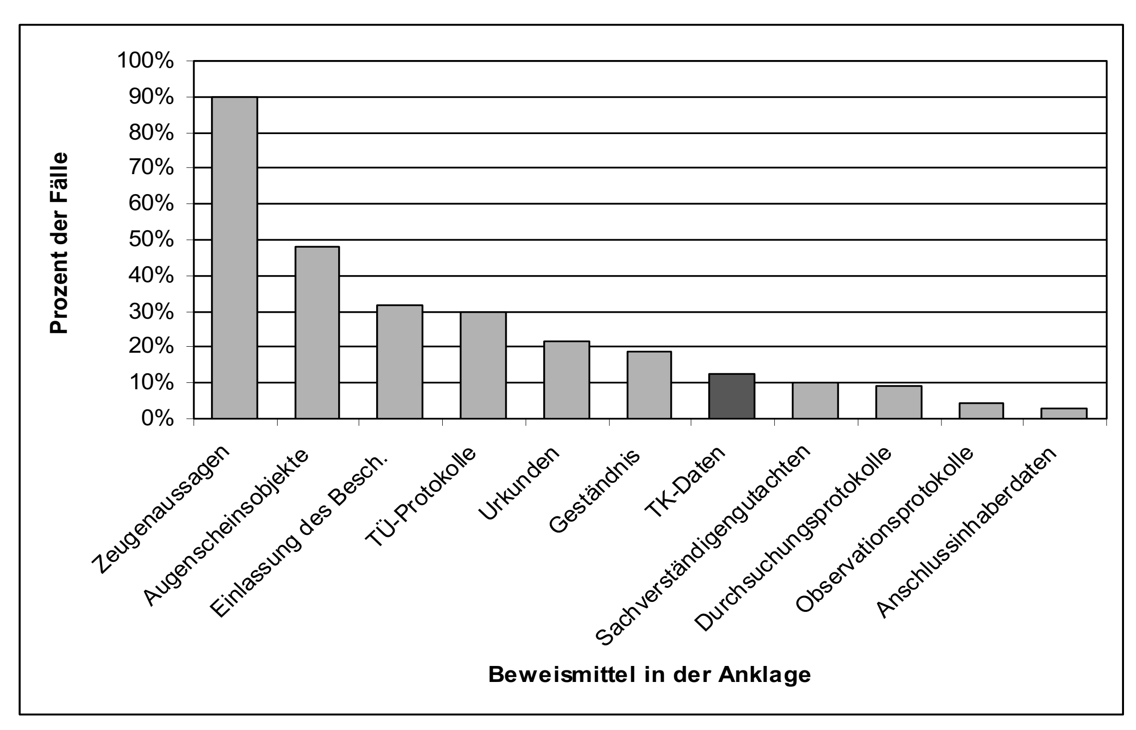
c) Stellenwert der Verkehrsdaten in der Anklage

In den 24 Anklageschriften, in denen die Verkehrsdaten erwähnt wurden, konnte bei 16 Anklagen ein hoher Stellenwert dieser Daten festgestellt werden. Der Akte war in diesen Fällen zu entnehmen, dass die Tat nur mit den Verkehrsdaten aufklärbar gewesen sei oder nur dadurch die Täterschaft des Beschuldigten nachweisbar gewesen sei. Es sei das entscheidende Beweismittel gewesen. Bei fünf Anklagen wurde den Daten zusammen mit anderen Beweismitteln (wie Zeugenaussagen oder Telefonüberwachung) Bedeutung zugewiesen. Bei zwei Anklagen nahm die Verkehrsdatenabfrage eine geringe Bedeutung ein. In einer Anklage war die Telefonüberwachung aufschlussreicher und in einem Fall wurde den Daten ein mittlerer Stellenwert zugewiesen.

In 34 Verfahren wurde die Verkehrsdatenermittlung zwar nicht in der Anklageschrift erwähnt, hatte aber bei fast der Hälfte der Fälle im Ermittlungsverfahren eine erhebliche Bedeutung. In der Anklage spielte sie aber keine Rolle mehr. In zehn Fällen wurde in der Anklage allgemein von Telekommunikationsüberwachungsmaßnahmen gesprochen, von welchen die Verkehrsdatenabfragen umfasst werden. Hier war nicht ersichtlich, welche Rolle die Verkehrsdaten gespielt haben. In fünf Fällen war ersichtlich, dass durch die Verkehrsdaten das Geständnis herbeigeführt wurde, welches dann in der Anklage als Beweismittel verwendet wurde. Wenn die Verkehrsdaten in der Anklage überhaupt erwähnt wurden, dann nahmen sie also meist einen hohen Stellenwert ein.

Abbildung 124

Beweismittel in der Anklage



d) Verkehrsdaten als Beweismittel in der Hauptverhandlung

Die Bedeutung der Verkehrsdaten in der Hauptverhandlung selbst ist äußerst gering. Bei 189 Beschuldigten kam es zu einer Hauptverhandlung. In 11 Prozent der Hauptverhandlungen wurden die Verkehrsdaten als Beweismittel in die Hauptverhandlung eingeführt. In diesen Fällen wurden sie zum Tatnachweis, zum Nachweis von Kontakten und Verbindungen zwischen den Tatbeteiligten sowie zur Standortfeststellung des Beschuldigten zur Tatzeit und zur Widerlegung von Aussagen verwendet. Beweisanträge, die sich auf die Verkehrsdaten bezogen, erfolgten von Seiten der Staatsanwaltschaft nie. Die Verteidigung stellte drei Verkehrsdaten-bezogene Anträge. In 40 Prozent der Fälle, in denen Verkehrsdatenabfragen explizit in der Anklage erwähnt wurden, wurden sie auch in der Hauptverhandlung als Beweismittel verwendet.

e) Verkehrsdaten als Beweismittel im Urteil

Auch im Urteil spielen die Daten keine besondere Rolle mehr. In 14 Prozent der Urteile (24 Nennungen) wurden die Verkehrsdaten in der Beweiswürdigung erwähnt. In diesen Fällen waren die Verkehrsdaten entweder alleine belastend (elf Nennungen) oder im Zusammenhang mit anderen Beweismitteln belastend (13 Nennungen). In den Fällen, in denen die Verkehrsdaten als Beweismittel im Urteil erwähnt wurden, hatten sie fast immer einen hohen (elf Nennungen) oder mittleren (sieben Nennungen) Stellenwert.

3. Experteninterviews

a) Polizeibeamte

In Bezug auf die Bedeutung der Daten für das weitere Verfahren gaben fast alle der befragten Polizeibeamten an, dass damit in den meisten Fällen ermittlungsunterstützende und tataufklärende Beiträge erlangt werden konnten. Die Maßnahme nehme einen hohen Stellenwert ein. Häufig seien gerade die Verkehrsdaten der „Schlüssel zur Lösung“ und der entscheidende Punkt in den Ermittlungen. Es handle sich nicht nur um begleitende und absichernde Maßnahmen. Die Daten seien häufig ein wesentliches Beweismittel und ein Indiz, das zu weiteren Ermittlungen führe. Die Daten seien für die Vorbereitung eines Verfahrens und zur Vorbereitung anderer Maßnahmen, wie einer Telekommunikationsüberwachung, unverzichtbar. Gerade in der Kombination mit einer anschließenden Telekommunikationsüberwachung sei die Verkehrsdatenabfrage ein erfolgversprechendes Mittel, das sich durch eine sehr hohe Erfolgsquote auszeichne. Vor allem mit der Funkzellenabfrage lassen sich nach Auskunft von Interviewpersonen herausragende Erfolge erzielen. Die Erfolgsaussichten würden aber dadurch etwas schwinden, dass die Täter mittlerweile die Ermittlungsmöglichkeiten kennten und von der Nutzung von Mobiltelefonen absehen würden. Damit sind Anpassungsprozesse angesprochen, die jedenfalls rationalen Kalkülen entsprechen und vor allem in Ermittlungen wegen Transaktionskriminalität Auswirkungen in Form von Selektionseffekten (in der Gruppe der beschuldigungsfähigen Täter) haben dürften.

b) Staatsanwälte

Im Hinblick auf die Bedeutung der Daten für das weitere Verfahren wird von etwa der Hälfte der befragten Staatsanwälte eine hohe Bedeutung angenommen. Die Daten seien häufig der einzige Ermittlungsansatz. Ohne die Verkehrsdatenabfrage könnten Delikte teilweise nicht aufgeklärt werden. Manchmal seien auch die Verkehrsdaten alleine ausreichend. Wenn anhand der Verkehrsdaten nachgewiesen werden könne, dass der Verdächtige sich am Tatort befunden habe und z. B. ein zusätzlicher Beweis bei der Durchsuchung gefunden werde, dann entstehe eine Beweislage, die so erdrückend sei, dass zumeist ein Geständnis erfolge. Weiter wurde angegeben, dass die Daten auch für das weitere Verfahren von großer Bedeutung seien. Die Daten seien im Regelfall Grundlage und Voraussetzung für weitere Ermittlungen. Teilweise gaben die Befragten an, dass die Maßnahme hauptsächlich im Ermittlungsverfahren wichtig sei. Die Daten könnten dem Beschuldigten vorgehalten werden und Anhaltspunkte für weitere Ermittlungen liefern. In der Hauptverhandlung würden die Daten dagegen i. d. R. keine große Bedeutung haben, meint die Hälfte der befragten Staatsanwälte. Aufgrund der Daten würden weitere Ermittlungen geführt, aus denen dann Beweismittel resultierten. Damit wird eine indirekte Rolle der Verkehrsdaten angesprochen. Auch hier wird auf die geständnisfördernde Wirkung der Verkehrsdaten verwiesen. Andere Beweise, die ggf. erst durch die Verkehrsdatenabfrage erlangt würden, würden aber eine größere Rolle spielen. Nur im Bestreitensfall würden die Daten auch noch in der Hauptverhandlung eine Rolle spielen.

c) Richter

Von den befragten Richtern wurde der Erfolg im Hinblick auf die Bedeutung der Daten teilweise als hoch eingeschätzt. Häufig sei es ein Beitrag zur Aufklärung der Tat. Weiter wurde auf den Wert als objektives Beweismittel hingewiesen. Man könne Aussagen kontrollieren. Außerdem wird wie von anderen Berufsgruppen angeführt, dass durch Verkehrsdaten eine erhebliche Motivation der Beschuldigten zur Einlassung und zum Geständnis ausgelöst werden könne. Ein weiterer Befragter unterscheidet zwischen verschiedenen Anwendungsbereichen. Bei E-mail-Accounts sei die Abfrage der Daten in „nahezu 100 Prozent“ der Fälle erfolgreich (Betrugsfälle bei Ebay). Ebenso sei die Standortfeststellung relativ erfolgreich. Von allen §§ 100g, 100h-Maßnahmen würden aber höchstens ein Drittel zu einem Ermittlungsergebnis und zur Anklage führen. Ein Befragter schätzt den Erfolg wegen der Masse an Mobiltelefonen als nicht besonders hoch ein. Im Ermittlungsverfahren spiele die Maßnahme freilich eine große Rolle. Die Daten würden der Abrundung des Tatbildes dienen. In der Hauptverhandlung und im Urteil würden die Daten aber keine unmittelbare Bedeutung mehr haben, führt einer der befragten Richter aus. Sie würden von anderen Beweismitteln überlagert.

d) Verteidiger

Die Bedeutung der Verkehrsdatenabfrage wird auch von den befragten Verteidigern überwiegend als hoch für das Ermittlungsverfahren, aber als geringfügig für die Hauptverhandlung eingeschätzt. Im Ermittlungsverfahren hätten die Daten massive Bedeutung, da sie erhebliche weitere Ermittlungen nach sich zögen. In der Hauptverhandlung würden Verkehrsdaten aber als Beweise keine große Rolle mehr spielen, hätten nur eine Indizfunktion und würden „Brücken“ zu anderen Beweismitteln bauen. In die Hauptverhandlung würden hauptsächlich andere Beweismittel eingeführt. Oft sei die Verkehrsdatenabfrage ein Einfallstor im Ermittlungsverfahren, die einen Überblick verschaffe und – wie auch von anderen Berufsgruppen betont – ggf. weitere Ermittlungsmaßnahmen auslöse. Weil die Verkehrsdatenabfrage schnell und kostengünstig sei, werde zunächst eine Maßnahme nach §§ 100g, 100h StPO und in der Folge eine solche nach §§ 100a, 100b StPO angeordnet. Um die Beweislage zu verfestigen, finde dann noch eine Observation oder eine Durchsuchung statt. Die eigentlichen Beweismittel würden durch diese klassischen Methoden (Observation, Durchsuchung) gesichert. Im Übrigen, und hier decken sich die Einschätzungen der Strafverteidiger mit denen der anderen Berufsgruppen, gebe der Beschuldigte – mit der Beweislage konfrontiert – schnell ein Geständnis ab.

4. Zusammenfassung der Ergebnisse

Im weiteren Verfahrensverlauf, d. h. nach Abschluss des Ermittlungsverfahrens haben die Verkehrsdaten keine besondere Bedeutung mehr. Dies ergibt sich sowohl aus der Aktenanalyse als auch aus den Gesprächen mit den Experten.

Bis zur Anklageerhebung kann den Akten noch ein gewisser Zusammenhang mit der Anklageerhebung und der erfolgreichen Abfrage der Verkehrsdaten entnommen werden. In den Fällen, in denen die Verkehrsdatenabfrage als erfolgreich eingestuft wurde, waren Anklagen sehr viel häufiger zu verzeichnen. Je weniger erfolgreich die Verkehrsdatenabfrage war, desto höher liegt die Einstellungsquote.

Als Beweismittel in der Anklageschrift spielen Verkehrsdaten eine eher untergeordnete Rolle. In 13 Prozent der Fälle (24 Anklagen) wurden die Verkehrsdaten in der Anklageschrift erwähnt. Bei 16 dieser Anklagen wurde den Daten allerdings ein hoher Stellenwert zugemessen. Die Daten waren nach den Ratings der Bearbeiter ausschlaggebend für den Nachweis der Täterschaft. Wenn die Daten in der Anklage also überhaupt erwähnt wurden, hatten sie meist eine hohe Bedeutung. In der Hauptverhandlung und im Urteil ist die Bedeutung der Daten relativ gering. In 11 Prozent der Hauptverhandlungen wurden die Verkehrsdaten als Beweismittel eingeführt (40 Prozent der Fälle, in denen sie explizit in der Anklageschrift erwähnt waren). Hier wurden sie u. a. zum Tatnachweis, zum Nachweis von Verbindungen, zur Standortfeststellung sowie zur Widerlegung von Aussagen verwendet. In 14 Prozent der Urteile (24) wurden die Daten in der Beweiswürdigung erwähnt. In diesen Fällen waren die Daten entweder allein oder im Zusammenhang mit anderen Beweismitteln belastend. Sie hatten fast immer einen hohen oder mittleren Stellenwert.

Die interviewten Praktiker weisen den Maßnahmen im Ermittlungsverfahren meist einen sehr hohen Stellenwert zu. Die Daten seien häufig der einzige Ermittlungsansatz. Sie würden der Vorbereitung anderer Maßnahmen dienen, aber auch alleine eine so erdrückende Beweislast bewirken, dass der Beschuldigte ein Geständnis abgebe. In der Hauptverhandlung dagegen würden die Daten keine große Rolle spielen. Die Daten hätten bereits zu anderen Ermittlungsmaßnahmen geführt, die dann zu Beweismittel führten, die wiederum eine stärkere Beweiskraft entfalteten. Nur im Bestreitensfall komme es vor, dass die Daten auch noch in der Hauptverhandlung erörtert werden.

5. Zusammenfassung, Diskussion der Ergebnisse und Empfehlungen

A. Fragestellungen

Die vorliegende Untersuchung hat die Evaluation der Nutzung von Verkehrsdaten der Telekommunikation im Strafverfahren zum Gegenstand. Die Fragestellungen der Untersuchung lassen sich im Einzelnen wie folgt zusammenfassen:

- Antrags- und Anordnungspraxis der Auskunftserteilung,
  - Grunddaten zur Praxis der Anordnungen
    - Anzahl der Betroffenen
    - Anlass und Ergebnisse der Maßnahmen
    - welche Straftaten liegen den Anordnungen zugrunde (insbesondere: sind Kinderpornographie, Organisierte Kriminalität und Rauschgiftdelikte die anlassgebenden Delikte?)
- Nutzung der erteilten Auskünfte
- (Beurteilung der) Effizienz der Verkehrsdatenabfrage (auch in Kombination mit anderen Ermittlungsmaßnahmen)
- Verhältnis der Verkehrsdatenabfrage zu anderen Ermittlungsmethoden
- Berücksichtigung der Anordnungsvoraussetzungen (insbesondere Begründung der Maßnahme)
- Verhältnismäßigkeit und Subsidiarität
- Implementation der Regeln über die Einhaltung der Benachrichtigungs- und Vernichtungspflichten
- Rechtliche und praktische Anwendungsprobleme
- Schwächen und Unklarheiten der Normen der §§ 100g, 100h StPO
- Ablauf der Anforderung von Verkehrsdaten und die Interaktionen zwischen Strafverfolgungsbehörden und Telekommunikationsanbietern
- Auswirkungen der Maßnahmen für die Netzbetreiber wie beispielsweise die bei der Durchführung entstehenden Kosten
- Kosten der Abfrage und Kostenersatz

B. Bisheriger Forschungsstand

Die Bedeutung empirischer Implementations- und Evaluationsforschung wird auf europäischer und nationaler Ebene hervorgehoben. Evaluationsanforderungen sind mit der Europäische Richtlinie zur Vorratsspeicherung (RL 2006/24/EG) ebenso verbunden wie mit dem vorliegenden Gesetzesentwurf der Bundesregierung zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckten Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (Bundestagsdrucksache 16/5846). Jedoch waren die bisherigen rechtspolitischen Entwicklungen im Bereich der Verkehrsdaten nicht auf aussagekräftige empirische Untersuchungen gestützt. Der empirische Forschungsstand lässt sich wie folgt zusammenfassen:

- Die Forschungslage ist defizitär. Aussagekräftige Daten zur Struktur der Anwendung und zu den Folgen der Abfrage von Verkehrsdaten liegen bislang nicht vor.
- Die bisherigen empirischen Studien beruhen auf einer (nicht nachvollziehbaren) Selektion oder auf einer gezielten (und interessengeleiteten) Auswahl bzw. auf einer Stichprobenziehung, die an der Überwachung des Telekommunikationsinhalts anknüpft.
- Weit verbreitet ist im Kontext des Gesetzgebungsprozesses die Einzelfallanalyse, die freilich Grundlagen für begründete Entscheidungen nicht liefern kann.
- Die aus den (hier weit gefassten) empirischen Ansätzen resultierenden Befunde verweisen darauf, dass die Nutzung von TelekommunikationsVerkehrsdaten auf kurze Zeiträume konzentriert ist.
- Die quantitative Bedeutung der Verkehrsdatenabfrage ist erheblich und liegt überall dort, wo eine statistische Erfassung durchgeführt wird, deutlich über den Zahlen der Überwachung der Telekommunikationsinhalte.
- Ausweislich schriftlicher Befragungen von Regierungen (und anderer Stellen) ergibt sich ein gemischtes Bild. Während aus einigen europäischen Ländern keine Probleme mit der derzeitigen Rechtslage zur Verkehrsdatenspeicherung mitgeteilt werden, verweisen andere auf das Problem von Löschungen und hierdurch vereitelter Ermittlungsmaßnahmen.
- Das Spektrum der Delikte, bei denen in der Praxis die Abfrage von Verkehrsdaten genutzt wird, hängt von der in der jeweiligen Untersuchung verwendeten Auswahl ab.
- Jedenfalls dürfte für die Verkehrsdatenabfrage ein sehr viel weiteres Deliktsfeld in Betracht kommen als für die Überwachung der Inhalte der Telekommunikation.
- Für Deutschland zeigt die frühere Praxis gemäß § 12 FAG, dass Zielsetzungen bei Abfragen der verbindungs- oder Bestandsdaten in der Regel nicht dokumentiert werden. Freilich lassen die Daten den Schluss darauf zu, dass Beziehungen zwischen Beschuldigten und dritten Personen bzw. die Identifizierung von Personen und Anschlüssen bekannter Personen im Vordergrund stehen.
- Kostenschätzungen lassen ganz erhebliche Varianz erkennen, die von erheblichen finanziellen Belastungen

von Telekommunikationsprovidern (vor allem durch die Investitionen in Struktur- und Unterhaltungsmaßnahmen zu Überwachungssystemen) bis zu kaum spürbaren Investitionen reicht.

– Offensichtlich wird die Verkehrsdatenabfrage in der Strafverfolgungspraxis und in der Rechtspolitik als eine im Vergleich zu der Telekommunikationsüberwachung wenig eingreifende Maßnahme angesehen.

C. Entwicklung der Bestands- und Verkehrsdatenabfrage in Deutschland

Die Anzahl der Anordnungen nach §§ 100g, 100h StPO hat von 2002 bis 2005 stark zugenommen. Vor allem von 2004 auf 2005 ist ein hoher Anstieg der Verkehrsdatenabfragen zu beobachten. Die Zahl der Beschlüsse, die eine Abfrage zu einer IMEI-Nummer (International Mobile Equipment Identity) beinhalteten, stieg bei einzelnen Anbietern etwa um das Vierfache, die angeordneten Zielwahlsuchen haben sich verdreifacht. Auf der Grundlage der uns von den Telekommunikationsanbieter-Unternehmen zur Verfügung gestellten Daten kann die Anzahl der Beschlüsse nach §§ 100g, 100h StPO geschätzt werden. Unter Berücksichtigung der Fehlerspanne bei Hochrechnungen lag die Zahl der Verkehrsdatenabfragen im Jahr 2005 bei etwa 40 000 (ohne Abfrage der Zuordnung von IP-Adressen). Die Tendenz ist stark ansteigend. Mit der schnellen Verbreitung mobiler Kommunikation ist die Verkehrsdatenabfrage zu einer weit verbreiteten, und die Bedeutung der Überwachung der Kommunikationsinhalte quantitativ übersteigenden Ermittlungsmaßnahme geworden.

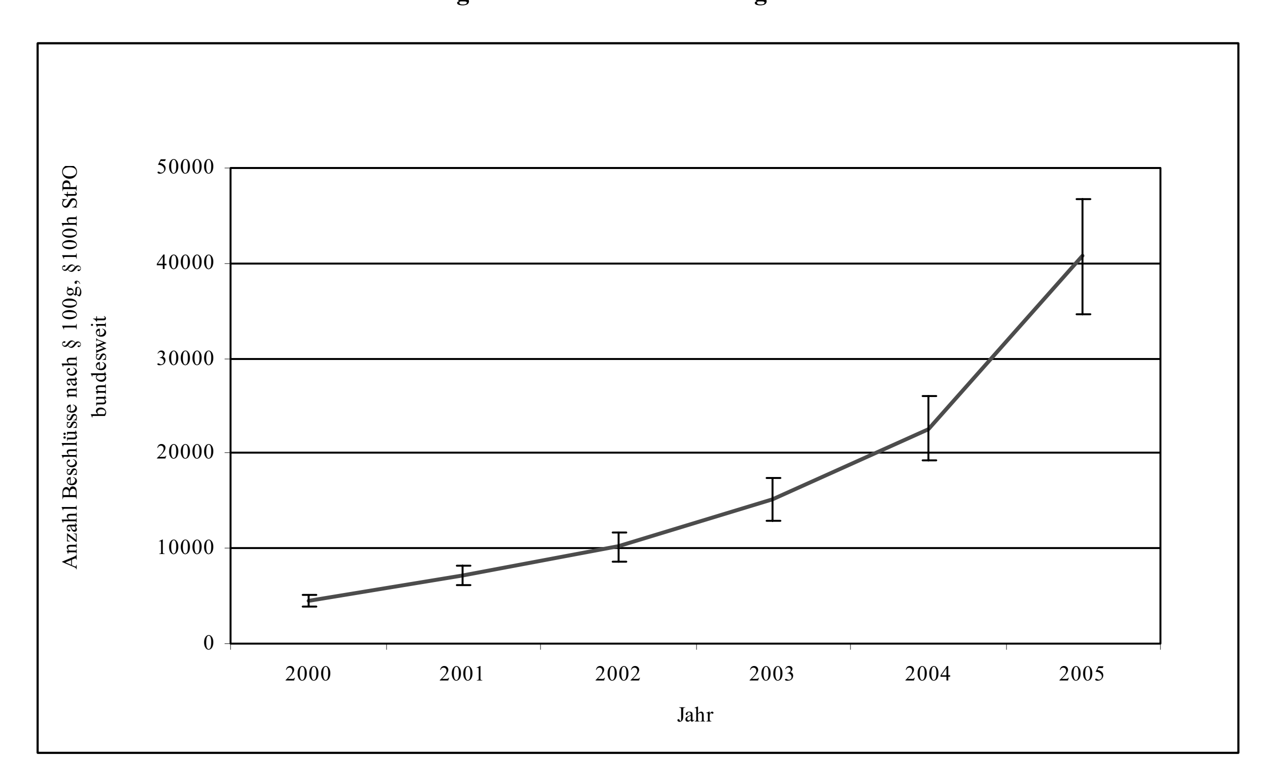
Dies gilt auch für die Bestandsdatenabfrage. Im Jahr 2006 belief sich die Zahl der Abfragen aus der zentralen Bestandsdatenbank der Telekommunikation durch Sicherheitsbehörden auf 3,6 Millionen. Die Entwicklungen in Bestandsdatenabfragen zeigen auch an, dass die konventionellen Register der Meldebehörden und Kraftfahrzeugverwaltung zwar nicht ihre Bedeutung verlieren. In den Vordergrund schieben sich freilich zentrale Kommunikationsanschlussinformationssysteme.

D. Untersuchungsmethoden

Die Untersuchung beruht auf einem Mehrmethodenansatz in Form von Aktenanalyse, Befragung und Interview. Damit wird auf die spezifische Mischung von Fragen reagiert, die neben (nur) aus Verfahrensakten entnehmbaren Informationen, Beobachtungen und Einschätzungen von Praktikern verlangen. Die Folgenabschätzung verlangt zudem eine möglichst umfassende (und unterschiedliche Perspektiven erfassende) Erhebung von Informationen, die als Indikatoren für Folgen der Abfrage von Verkehrsdaten genutzt werden können. Solche Indikatoren können nur aus einer Kombination von Strafverfahrensakten,

Abbildung 125

Entwicklung der Verkehrsdatenabfragen 2000 bis 2005



Befragung und Interview entstehen, da eine direkte Beobachtung der relativen Bedeutung der Ermittlungsmaßnahme nicht möglich ist. Eine direkte Beobachtung setzt ein kontrolliertes Experiment voraus, in dem die Rahmenbedingungen gleich gehalten und lediglich die Interventionen variiert werden. Ein solches kontrolliertes Experiment kann für die Beurteilung der Verkehrsdatenabfrage nicht durchgeführt werden. Die Bildung von Kontrollgruppen, die in anderen Bereichen strafrechtlicher Interventionen (insbesondere strafrechtlicher Sanktionen) einen, wenn auch nicht gleichwertigen, Ersatz für kontrollierte Experimente schafft, ist im Feld der empirischen Strafverfahrensforschung jedenfalls dann nicht möglich, wenn es um verdeckte Ermittlungsmethoden geht. Dies zeigt im Übrigen auch die MPI-Studie zur Telekommunikationsüberwachung, in der der Versuch unternommen wurde, eine Kontrollgruppe von Betäubungsmittelstrafverfahren und anderen Verfahren, die nicht einer Überwachung der Kommunikation ausgesetzt waren, zu bilden. Die durch den Einsatz verdeckter Ermittlungsmethoden erzeugten Kombinationen von Ermittlungsmaßnahmen führen aber zu einer Situation, die vergleichbare Fälle (und damit eine Kontrollgruppe von nicht der verdeckten Ermittlungsverfahren ausgesetzten Verfahren) nicht mehr entstehen lässt. Es bleibt deshalb allein die Identifizierung geeigneter Indikatoren des Nutzens (und der Kosten), die sich aus Dokumentenanalyse, Befragung und Interview ziehen lassen und die aus unterschiedlichen Perspektiven und auf unterschiedliche Dimensionen des Verfahrens bezogen, ferner in der Kombination qualitativer und quantitativer Zugänge vergleichende Beurteilungen der Folgen erlauben.

Die **Aktenanalyse** umfasst die Auswertung von Verfahrensakten aus den Jahren 2003 und 2004 aus den Bundesländern Baden-Württemberg, Berlin, Mecklenburg-Vorpommern und Nordrhein-Westfalen. Da die Justizbehörden keine separate Statistik über die Anordnungen nach §§ 100g, 100h StPO führen, wurden die Aktenzeichen aus den §§ 100g, 100h-Beschlüssen bei den führenden Telekommunikationsanbietern Arcor, E-Plus, O_2, T-Com, T-Mobile und Vodafone erhoben. Der Aktenauswertung liegen 467 Verfahren zugrunde. Die Anzahl der Verfahren verteilt sich etwa gleich auf die vier Bundesländer, aus denen die Akten angefordert wurden. 27 Prozent der Verfahren kommen aus Baden-Württemberg, 22 Prozent aus Berlin, 27 Prozent aus Mecklenburg-Vorpommern und 24 Prozent aus Nordrhein-Westfalen.

Ein zweites Modul der Untersuchung betrifft die **schriftliche Befragung** von Staatsanwälten auf der Basis einer Totalerhebung bei Staatsanwaltschaften in Deutschland. Die Rücklaufquote beträgt 19 Prozent. Diese liegt im Rahmen der in schriftlichen Befragungen erzielbaren Quoten. Die Bundesländer unterscheiden sich zwar in den Rücklaufraten. Jedoch werden in fast allen Bundesländern die Landgerichtsbezirke und damit die Staatsanwaltschaften annähernd komplett abgedeckt. Ferner liegen auch aus den Bundesländern Nordrhein-Westfalen und Bayern Fragebögen aus einer solchen Anzahl von Staatsanwaltschaften vor, die es erlaubt, davon auszugehen, dass die Variationsbreite von Einstellungen und Wahrnehmungen innerhalb der jeweiligen Staatsanwaltschaft im Hinblick auf die Praxis der Verkehrsdatenabfrage abgebildet wird.

Ein drittes Untersuchungsmodul stützt sich auf **Experteninterviews** (bzw. Interviews mit Schlüsselpersonen). Gespräche wurden mit 53 Personen geführt. Dabei handelt es sich um zehn (Ermittlungs-)Richter, 13 Staatsanwälte, 16 Polizeibeamte, vier Strafverteidiger, sechs Telekommunikationsanbieter und vier Datenschutzbeauftragte (aus den durch die Aktenuntersuchung erfassten Bundesländern).

E. Ergebnisse der Untersuchung

I. Verkehrsdatenabfragen im Spiegel von Telekommunikationsunternehmensdaten

Die zur Stichprobenziehung herangezogenen Datensätze der Telekommunikationsunternehmen erlauben einen allgemeinen Einblick in Struktur und Eingriffsbreite der Verkehrsdatenüberwachung. Auf der Basis der auf drei Monate bezogenen Daten zweier Unternehmen ergibt sich, dass die Abfragen fast ausschließlich auf die Vergangenheit gerichtet sind. Am häufigsten sind Beschlüsse betreffend den so genannten Zielsuchlauf nach eingehenden Anrufen (60 Prozent), gefolgt von kombinierten Auswertungen ab- und eingehender Anrufe (22,5 Prozent). Die Funkzellenabfrage betrifft knapp 18 Prozent der Beschlüsse. Die letztere zeichnet sich durch ihre Kurzzeitigkeit von durchschnittlich fünf Stunden, mehrheitlich sogar weniger als einer Stunde aus. Auf eine etwas längere Dauer ist die Zielwahlsuche angelegt, während die breit angelegte systematische Erfassung der Kommunikation mit einer Dauer von zwei bis drei Monaten als ganz anders ausgestalteter Ermittlungsansatz erscheint. Eingesetzt werden die Maßnahmen bei Abfragen im Festnetz vorwiegend im Betrugsbereich (30 Prozent), bei Raub und Mord (jew. ca. 10 Prozent) sowie bei Betäubungsmitteldelikten (8 Prozent). Ganz anders stellt sich die Situation im Internet dar. Zwar liegt auch hier der Betrug an erster Stelle (>40 Prozent). Eine nennenswerte Rolle spielen daneben dann Kinderpornogaphie (knapp 30 Prozent) und Urheberrechtsverletzungen.

Die Analyse der Eingriffsbreite ergibt zunächst, dass die meisten Kontakte durch die kombinierte Überwachung erfasst werden. Nach der Eliminierung von zwei Extremfällen ergibt sich ein Durchschnitt von 357 Gesprächen. Bei der Funkzellenabfrage liegt die Anzahl bei 282. Insgesamt führt die Funkzellenabfrage im Durchschnitt zu der Registrierung von 111 verschiedenen Mobilfunkteilnehmern innerhalb der Funkzelle (repräsentiert durch die abgehenden Anrufe) und 183 Nummern dort eingehender Telefonate. Bei einer Hochrechnung ergibt sich für das Jahr 2005, dass insgesamt etwa zwei Prozent aller Mobilfunkteilnehmer von einer Funkzellenabfrage betroffen waren. Weitaus geringer ist hingegen die Erfassungsbreite der Zielwahlsuche. Mit ihr werden im Durchschnitt nur 2,5 Kommunikationsteilnehmer erfasst; bei mehr als 95 Prozent aller Maßnahmen sind weniger als zehn Teilnehmer betroffen.

II. Anordnungspraxis der Verkehrsdatenabfrage: Struktur, Typ und Betroffene

Aus den in die Untersuchung fallenden 467 Verfahren folgen 1 257 Beschlüsse zur Abfrage von Verkehrsdaten. Diese Beschlüsse betrafen 1909 Anschlüsse, denen wiederum 1 645 Anschlussinhaber (505 Tatverdächtige und 1 110 Dritte, 70 Prozent) zugeordnet werden konnten. Darüber hinaus konnten 1 709 Anschlussnutzer festgestellt werden, wobei in über 40 Prozent der Fälle der Beschuldigte alleiniger Nutzer war. Dritte von der Verkehrsdatenabfrage betroffene Anschlussinhaber waren überwiegend das Opfer der Straftat sowie Familienangehörige des Beschuldigten. In keinem Verfahren war den Akten zu entnehmen, dass ein Berufgeheimnisträger Betroffener der Maßnahme war. Zeugnisverweigerungsberechtigte deckten sich mit Angehörigen des Tatverdächtigen. Zu zwei Dritteln wurden ein- oder abgehende Daten von oder zu Mobilfunkanschlüssen erhoben (66 Prozent). 25 Prozent der betroffenen Anschlüsse waren private Festnetzanschlüsse. Betriebliche Festnetzanschlüsse waren dagegen nur zu 3,8 Prozent Ziel der Maßnahmen. Fax und E-Mail waren nur in Ausnahmefällen betroffen. In den Beschlüssen wurden überwiegend (93 Prozent) (auch) bereits gespeicherte Daten abgefragt. Die Zielwahlsuche wurde in 55 Prozent der Beschlüsse angeordnet. In die Zukunft gerichtet waren 33 Prozent der Abfragen. Standortabfragen (18 Prozent) wurden etwa doppelt so häufig angeordnet wie Funkzellenabfragen (10 Prozent der Fälle). Insgesamt wurden Diensteanbieter durch die 1 257 Beschlüsse in 3095 Fällen gemäß §§ 100g, 100h StPO zur Übermittlung von Daten verpflichtet. Pro Beschluss sind damit durchschnittlich knapp drei Telekommunikationsfirmen betroffen.

III. Erfasste Delikte

Die Verfahrensakten zeigen, dass 70 Prozent der Beschlüsse nach §§ 100g, 100h StPO ausschließlich Katalogdelikte des § 100a Satz 1 StPO betreffen. Schwerpunkte bilden bei denv Katalogstraftaten Betäubungsmittel- (26 Prozent), Raub- (25 Prozent), Tötungsdelikte (19 Prozent) sowie Bandendiebstahl (10 Prozent). Bei den anderen Straftaten (mittels Endeinrichtung oder von erheblicher Bedeutung) stehen Ermittlungen wegen schweren Diebstahls (29 Prozent) und Betrugsdelikten (27 Prozent) im Vordergrund. Einfache Diebstähle lagen in 5 Prozent der Fälle zugrunde. Die einfachen Diebstähle beziehen sich (ebenso wie Straßenraub) überwiegend auf Mobiltelefone, der Betrug etwa zur Hälfte auf Endeinrichtungsstraftaten (Enkeltrick). In 85 der ausgewerteten Verfahren (18 Prozent) fanden sich Hinweise auf Elemente der Organisierten Kriminalität. Verfahren wegen Kinderpornografie fielen nicht in die Stichprobe. Schon die allgemeinen Verteilungen der die Ermittlungsverfahren begründenden Straftatbestände sprechen demnach dafür, dass sich die Verkehrsdatenabfrage auf ein weites Deliktsspektrum bezieht, dass also nicht der Telekommunikationsüberwachung entsprechende Konzentrationen bei Transaktionsdelikten (insbesondere Betäubungsmittelstraftaten) beobachtet werden können, und dass von daher die Verkehrsdatenabfrage von der Phänomenologie der Delikte her gesehen als weit greifendes Ermittlungsinstrument angesehen werden kann. Dies deckt sich im Kern mit den Befunden aus der Untersuchung des Bundeskriminalamts aus dem Jahr 2005 und mit der Struktur der Erledigungen sowie Sanktionen, die sich aus der Aktenanalyse abbilden lässt. Die Sanktionsstruktur spricht dafür, dass ein bedeutsamer Anteil der Verfahren allenfalls der mittleren Kriminalität zuzuordnen ist. Werden Einstellungen nach § 170 II StPO ausgeschlossen, die Geringfügigkeitseinstellungen einbezogen und Geldstrafen, Bewährungsstrafen und Rechtsfolgen des JGG ohne Jugendstrafe zu diesem Bereich der nicht über eine mittlere Schwere hinausgehenden Kriminalität gerechnet, dann beziehen sich die Verfahren hierauf zu knapp 60 Prozent. Die Informationen aus der Befragung und aus den Interviews fügen sich in eine solche Betrachtungsweise ein. Die Verkehrsdatenabfrage ist (mit Ausnahme von Verkehrs- und Wirtschaftsdezernaten) auf dem Wege zu einer für fast alle Deliktsbereiche eingesetzten Ermittlungsmaßnahme. Sie allerdings stark bedingt durch die Tatphänomenologie (Täter-Opfer-Kontakte (letzter Kontakt bei Tötungsdelikten, Trickbetrug), Tatobjekte, Täterabsprachen und Netzwerke), die sich mit der technologischen Entwicklung gewandelt hat. Hinzu tritt, dass die Verkehrsdatenabfrage von Praktikern tendenziell als (im Vergleich zu konventionellen und anderen verdeckten Ermittlungsmaßnahmen) weniger belastend eingeordnet wird. Es fällt insoweit auf, dass die rechtspolitischen Debatten (große Sensibilisierung) und die Praktiken (Alltagsgeschäft) auseinanderfallen. Überwiegend wird von Befragten und Interviewten (aus den Bereichen Strafverfolgung und Justiz) für eine Beibehaltung der derzeitigen Voraussetzung der Straftat von erheblicher Bedeutung mit Verweis auf den Straftatenkatalog des § 100a Satz 1 StPO plädiert. Betont wird, dass die Regelung Flexibilität erlaube. Doch wird auch für die Beschränkung auf Straftaten von erheblicher Bedeutung votiert. Erwartungsgemäß sprechen sich Verteidiger, Datenschutzbeauftragte und Telekommunikationsunternehmen für einen festen Straftatenkatalog aus, mit der Zielsetzung der Reduzierung der Anordnungen einerseits und der Stärkung von Rechtssicherheit (Vorhersehbarkeit) andererseits.

IV. Einleitung, Entscheidungen und Begründungsstrukturen

Die Initiative zu Verkehrsdatenabfragen geht erwartungsgemäß fast ausschließlich (nach der Aktenanalyse zu 91 Prozent) von der Polizei aus. Die Bedeutung polizeilicher Initiativen wird auch durch die Ergebnisse der Befragung und Interviews unterstrichen. Eine besondere Rolle spielen offensichtlich Absprachen zwischen Polizei und Staatsanwaltschaft, die die Funktion haben, Fälle aussichtsreicher Antragstellung zu identifizieren. 90 Prozent der Verkehrsdatenabfragen werden nach den Ergebnissen der Aktenanalyse vom Ermittlungsrichter angeordnet, 10 Prozent erfolgen als Eilanordnungen. Richterliche Bestätigungen von staatsanwaltschaftlichen Eilanordnungen finden sich in 69 Prozent der Fälle. Eilanordnungen

werden im Übrigen ohne Bestätigung umgesetzt, soweit sich die Netzbetreiber der Herausgabe nicht entgegenstellen. Nach Ansicht der befragten Staatsanwälte und Richter bedarf es jedoch nur einer Bestätigung, wenn Daten über den Zeitraum der Bestätigungsfrist hinaus benötigt werden. Die beantragte **Dauer** der Maßnahmen entspricht ganz überwiegend der angeordneten Dauer. Dies zeigen sowohl die Ergebnisse der Aktenanalyse als auch die der schriftlichen Befragung. Übereinstimmend wird durch beide Module festgestellt, dass die Abfragedauer schwerpunktmäßig bei drei Monaten liegt. Darüber hinaus liegt ein weiterer Schwerpunkt auf Abfragen für Zeiträume innerhalb eines Tages. Die Abfrage vorhandener Daten bezieht sich überwiegend entweder auf einen Zeitraum innerhalb eines Tages oder auf die Dauer von drei Monaten. In die Zukunft gerichtete Abfragen konzentrieren sich auf eine Dauer von drei Monaten. Die Zielwahlsuche erfolgt schwerpunktmäßig innerhalb eines Tages oder für drei Monate. Bei dem Verdacht von Tötungs-, Raub- und Betäubungsmitteldelikten liegen Schwerpunkte auf der Abfrage von Daten aus der Vergangenheit. Dies wird bei Tötungsdelikten daran liegen, dass zunächst festgestellt werden soll, mit wem Opfer die letzten Kontakte hatten. Im Falle von Raubüberfällen kann (mittels Funkzellenabfrage) überprüft werden, wer im Bereich des Tatorts mit anderen telefonisch in Kontakt stand.

Die **Begründungen** (in Initiativen, Anträgen und Anordnungen) wurden auf der Grundlage einer Kategorienbildung, die derjenigen der MPI-Studie zur Telekommunikationsüberwachung entspricht, in Qualitätskategorien eingeordnet. Die so erfasste Qualität der Begründungen von Anregungen, Anträgen und Beschlüssen in den ausgewerteten Verfahren nimmt von der Anregung bis zum Beschluss ab. Während die Anregungen der Polizei noch zu 55 Prozent als substantiell bewertet wurden, ist dies bei den Anträgen der Staatsanwaltschaft nur noch zu 35 Prozent der Fall. Die Beschlussbegründungen wurden zu 25 Prozent als substantiell bewertet. Insbesondere fällt hier die formelhafte Wiedergabe des Gesetzestextes auf. Zudem werden die Anträge der Staatsanwaltschaft häufig vollständig in den Beschluss übernommen. Vor allem in Baden-Württemberg, aber auch teilweise in Mecklenburg-Vorpommern ist es üblich, dass die Staatsanwaltschaft einen vorformulierten Beschlussentwurf an das Gericht schickt, den der Richter nur noch zu unterschreiben braucht. Das Bild der Begründungen, so wie es sich aus den Verfahrensakten ergibt, ähnelt demjenigen, das in abgeschlossenen Untersuchungen von der Begründung der Telekommunikationsüberwachung gezeichnet wurde.

V. Verfahrenserledigungen: Einstellungen, Anklage, Urteil und Rechtsmittel

In 58 Prozent der Fälle wurde das Verfahren durch die Staatsanwaltschaft eingestellt und in 1 Prozent der Fälle erfolgte eine Teileinstellung. Anklage wurde in 21 Prozent der Fälle erhoben und ein Strafbefehlsantrag wurde in 2 Prozent der Fälle gestellt. Der Rest der Verfahren war entweder noch nicht abgeschlossen oder es kam zu einer Abtrennung. Die Einstellungen gehen erwartungsgemäß ganz überwiegend auf § 170 II StPO und dort auf Unbekanntsachen zurück. Von 211 Angeklagten wurden 85 Prozent verurteilt. Die Sanktionen entfallen zu 75 Prozent auf Freiheitsstrafen, wobei lange Freiheitsstrafen von mehr als fünf Jahren sowie lebenslänglich 16 Prozent ausmachen. Insoweit handelt es sich ganz offensichtlich bei den Straftaten, die unter die Verkehrsdatenabfrage fallen, einmal um schwere Kriminalität, zum anderen – und wie weiter oben angesprochen – um Straftaten, die in der Schwere deutlich unterhalb dieser Schwelle einzuordnen sind. Gegen Urteile wurden zu etwa 30 Prozent Rechtsmittel und Rechtsbehelfe eingelegt. Davon entfallen etwa 60 Prozent auf eine Revision und 25 Prozent auf eine Berufung. Der Rest betrifft Einsprüche gegen einen Strafbefehl. Die Einlegung von Rechtsmitteln führt zur Abänderung des Urteils in fünf Fällen und zur Aufhebung in drei Fällen. Ein Zusammenhang der Verkehrsdatenabfrage mit der Abänderung oder Aufhebung des Urteils konnte in keinem Fall festgestellt werden.

VI. Verhältnis der Verkehrsdatenabfrage zu anderen Ermittlungsmaßnahmen und Subsidiarität

Die Verkehrsdatenabfrage ist eine Maßnahme, die zu Beginn des Ermittlungsverfahrens eingesetzt wird und gleichzeitig in zwei Dritteln der Verfahren Grund für die erste Einschaltung der Staatsanwaltschaft. Der erste Beschluss ergeht in 51 Prozent der Verfahren innerhalb der ersten 14 Tage. Insoweit gibt es Parallelen zum Einsatz der Telekommunikationsüberwachung nach §100a StPO. Kombinationen mit anderen Ermittlungsmaßnahmen erfolgen nach Angaben der Befragten vor allem mit der Telekommunikationsüberwachung, aber auch mit der Durchsuchung und der Beschlagnahme. Dies wird durch die Aktenanalyse bestätigt. Telekommunikationsüberwachung und Verkehrsdatenabfrage werden kombiniert angewendet und im Verhältnis zueinander als Ergänzung angesehen. Die Verkehrsdatenabfrage dient dabei der Vorbereitung der Telekommunikationsüberwachung, durch Feststellung von Anschlussnummern, für die dann die Telekommunikationsüberwachung geschaltet wird, oder der Identifizierung von Gesprächsteilnehmern. Sie wird gleichzeitig mit der Telekommunikationsüberwachung angeordnet, wenn die Abfrage gespeicherter Daten und die gleichzeitige Anordnung der Telekommunikationsüberwachung für die Zukunft zu einem umfassenden Bild der Kommunikationsmuster führen soll. Hinzu treten in diesem Zusammenhang die aus Befragungen und Interviews folgenden Hinweise auf die Ökonomie der Verkehrsdatenabfrage (gerade im Verhältnis zur Telekommunikationsüberwachung). Im Übrigen wird der Verkehrsdatenabfrage vor allem die Funktion zugeordnet, erste Ermittlungsansätze zu gewinnen, um dann andere Maßnahmen durchführen zu können. Gerade die Verfahren, in denen es allein zu einer Verkehrsdatenabfrage kam, zeigen, dass es bei mittels Endeinrichtung begangenen Straftaten wie Betrug (Enkeltrick), Androhung von Straftaten oder dem Diebstahl oder Raub von Mobiltelefonen kaum andere Ermittlungsansätze als die Verkehrsdatenabfrage gibt. Im Übrigen deuten auch die Einsätze bei Tötungsdelikten und bei Betäubungsmitteldelikten darauf hin,

dass es sich hier eben nicht um das „letzte“ Mittel, sondern, umgekehrt, um das „erste“ Mittel handelt. Denn tatsächlich dürfte es bei den Ermittlungen gerade bei Tötungsdelikten zunächst darum gehen, abzuklären, mit welchen Personen das Opfer zuletzt in telefonischem Kontakt stand. Jedoch deuten die Ergebnisse insgesamt darauf hin, dass gerade die Veränderungen im Kommunikationsverhalten wohl dazu führen, dass sich – deliktsspezifisch – die Ansätze und Ansatzmöglichkeiten in den Ermittlungen so anpassen, dass eben nicht mehr von einer Konkurrenz der Ermittlungsmaßnahmen ausgegangen werden kann. Denn andere Möglichkeiten, das Telekommunikationsverhalten von Menschen für die Vergangenheit zu ermitteln, gibt es schlicht nicht. Insoweit ergibt sich eine nachvollziehbare Typologie des Verhältnisses der Verkehrsdatenabfrage zu anderen Ermittlungsmaßnahmen:

VDA bietet den einzigen Ermittlungsansatz (Tatobjekt Mobiltelefone, Tatbegehung führt über Telekommunikation);

VDA ergänzt zur Vergangenheit, insbesondere die TKÜ (Netzwerke, Beziehungen, weitere Tatbeteiligte), Überprüfungen anderer Beweismittel;

VDA bereitet vor, insbesondere TKÜ und Telekommunikationsraster;

VDA identifiziert Tatverdächtige, im Nachgang zu anderen Ermittlungsmaßnahmen oder als erste Maßnahme (Beispiel: Tötungsdelikte).

VII. Der Richtervorbehalt

Dem Richtervorbehalt wird bei verdeckten Ermittlungsmaßnahmen besondere Bedeutung beigemessen. In der Überprüfung der Umsetzung des Richtervorbehalts wurden verschiedene Kriterien überprüft. Zunächst ist, ähnlich den Befunden zur Telekommunikationsüberwachung, festzustellen, dass den Akten nur ganz selten Ablehnungen von Anträgen zu entnehmen sind (N = 5). Dies mag freilich auch eine Konsequenz der bereits angesprochenen Selektion durch Polizei und Staatsanwaltschaft sein. Auch Abänderungen der Anträge werden kaum vorgenommen. Bei 32 von 1909 Anschlüssen kam es zu Veränderungen überwiegend der Dauer der Maßnahme (Reduzierung) oder zu einer Konkretisierung. Dem entspricht die Einschätzung der befragten Staatsanwälte, die davon ausgehen, dass die angeordnete fast immer der beantragten Dauer entspricht. Die Verwendung von Vordrucken, die Übernahme von Antragsbegründungen der Polizei oder der Staatsanwaltschaft und formelhafte Begründungen werden ergänzt durch den Eindruck der Befragten, dass der Richtervorbehalt seine Funktion nicht in ausreichendem Maße erfülle. Verwiesen wird in diesem Zusammenhang auf die Arbeitsbelastung der Ermittlungsrichter und Prioritätssetzungen, die gefördert werden mag durch die Einschätzung, dass die Verkehrsdatenabfrage einen im Vergleich zu anderen Ermittlungsmaßnahmen weniger starken Eingriff mit sich bringe. Freilich zeigen die Befragungen und Interviews auch, dass ein effizienter Richtervorbehalt nachdrücklich eingefordert wird.

VIII. Benachrichtigung und Löschung

Benachrichtigung und Löschung von erhobenen Telekommunikationsdaten zeigen Probleme an. Nur für 4 Prozent der Beschlüsse war eine Benachrichtigung der Betroffenen in den Akten dokumentiert. Ganz überwiegend waren Benachrichtigungen jedenfalls in den Akten nicht enthalten. Die Beschuldigten konnten für 4 Prozent der Beschlüsse auf sonstige Weise Kenntnis erlangen und bei einem Drittel der betroffenen Beschuldigten war die Kenntnisnahme durch Akteneinsicht möglich. Die Befragungen und Interviews unterstreichen diese Befunde. Auch die Vernichtung der erhobenen Daten konnte den Akten nur in 3 Prozent der Verfahren entnommen werden. Die Vernichtung der Daten ist offensichtlich nicht die Regel, denn Staatsanwälte äußerten entweder, es sei nicht bekannt, ob die Vernichtung erfolge, oder, dass die Daten nicht vernichtet werden.

IX. Effizienz der Verkehrsdatenabfrage

Die Beurteilung der Effizienz ist wegen der skizzierten Beschränkungen der Untersuchungsanordnung lediglich über verschiedene Indikatoren durchzuführen. Hierfür wurden die mit der Verkehrsdatenabfrage verfolgten Ziele identifiziert, die aus den Akten entnehmbaren Erfolge dazu in Beziehung gesetzt, das Verhältnis zur Verfahrenserledigung analysiert und schließlich Einstellungen und Perzeptionen aus Befragung und Interviews einbezogen. Im Zielbereich der Verkehrsdatenabfragen steht die Identifizierung des noch unbekannten Täters im Vordergrund (40 Prozent). Es folgen die Ermittlung weiterer Tatbeteiligter bzw. ihrer Anschlüsse (30 Prozent) und die Sicherung von Beweisen (26 Prozent). Die Feststellung der Glaubwürdigkeit des Beschuldigten oder eines Zeugen wurde eher selten verfolgt (1 Prozent). Sonstige Ziele (5 Prozent) bezogen sich auf die Ermittlung von Liefer- und Absatzwegen, des Tatorts, von Bandenstrukturen, die Feststellung der Aufenthaltsorte der Mittäter, das Auffinden von geraubten Mobiltelefonen und die Ermittlung von Zeugen. Für 43 Prozent der Beschlüsse konnte aus den Akten eine Erfolgseinschätzung entnommen werden. In diesen Fällen wurde bei 18 Prozent der Beschlüsse die Verkehrsdatenabfrage in den Akten als erfolgreich eingeschätzt. 17 Prozent der Beschlüsse wurden in den Akten als bedingt erfolgreich und 65 Prozent als nicht erfolgreich bezeichnet. Diese Verteilungen sind angesichts des hohen Anteils an Unbekanntsachen und angesichts der Einstellungsrate erwartungsgemäß. Der am häufigsten für das Verfahren festgestellte konkrete Erfolg ist die Identifizierung des Beschuldigten (10,1 Prozent). Ebenfalls häufig sind die Feststellung weiterer Tatbeteiligter (6,6 Prozent), die Feststellung von Kommunikationspartnern des Beschuldigten (6 Prozent) sowie die Sicherung von Beweisen (5,6 Prozent). Ein weiterer Indikator für die Effizienz der Verkehrsdatenabfrage liegt im Ausgang des Verfahrens. In knapp 60 Prozent der Fälle wurde das Verfahren eingestellt. Anklage (mit Strafbefehlsanträgen) wurde in 23 Prozent der Fälle erhoben. Insoweit reflektiert die Verfahrenserledigung die bekannten Probleme der Ermittlungen in Unbekanntsachen. Wenn Anklage erhoben wurde, wurden die Angeklagten in 85 Prozent der

Fälle verurteilt. Teileinstellung und Teilfreispruch erfolgten zu jeweils 1 Prozent. Freigesprochen wurden die Beschuldigten in 6 Prozent der Fälle und in 7 Prozent der Fälle wurde das Verfahren gegen die Angeklagten durch das Gericht eingestellt. Zur Beurteilung der Effizienz kann nunmehr überprüft werden, wie das Verfahren abgeschlossen wurde, wenn die Verkehrsdatenabfrage erfolgreich bzw. nicht erfolgreich war. Die Daten zeigen, dass in den Fällen, in denen die Verkehrsdatenabfrage in den Akten oder von den Bearbeitern der Akte als erfolgreich eingestuft wurde, die Anklagequote im Vergleich zu den anderen Fallgruppen deutlich erhöht ist. Dementsprechend nimmt die Einstellungsquote mit der Erfolglosigkeit der Verkehrsdatenabfrage drastisch zu. Freilich handelt es sich damit um einen Indikator, mit dem eine Kausalität zwischen Verkehrsdatenabfrage und der Entscheidung über Anklage und Einstellung nicht hergestellt werden kann. Schließlich entfaltet die Verkehrsdatenabfrage Wirkungen überwiegend im Ermittlungsverfahren. Insoweit teilt sie Eigenheiten der verdeckten Ermittlungsmethoden. In der Hauptverhandlung spielen die Daten eine untergeordnete Rolle. Vor allem das bei Vorhalt von Verkehrsdaten erwirkte Geständnis des Beschuldigten wird von interviewten Praktikern der Strafverfolgung hervorgehoben, sowie die mehrfach erwähnte oder die nach der Verdachtserhärtung durch die Daten erfolgte Durchsuchung. In diesen Fällen würden die Daten dann nach dem Ermittlungsverfahren nicht mehr benötigt. Auch die Ergebnisse der Aktenauswertung bestätigen diese Einschätzung. Im Ermittlungsverfahren konnten sehr wichtige Hinweise durch die Abfrage der Daten erlangt werden. In Anklage, Hauptverhandlung und Urteil war die Verwendung der Daten jedoch relativ selten. Wenn sie allerdings in der Anklage aufgeführt wurden, nahmen sie in der Regel einen hohen Stellenwert ein. Für das Rechtsmittelverfahren spielen Verkehrsdatenabfragen nach Lage der Akten und ausweislich der Aussagen der Experteninterviews keine Rolle.

X. Interaktionen und Probleme in der Implementation

Untersuchungsgegenstand waren auch Interaktionen zwischen den verschiedenen, an dem Ablauf einer Verkehrsdatenabfrage Beteiligten und die Identifizierung von Problemen. Sowohl die Ergebnisse der Befragungen als auch die der Aktenanalyse zeigen, dass bei der Abfrage von Personendaten zu dynamischen IP-Adressen unterschiedliche Rechtsauffassungen vertreten werden und daher eine uneinheitliche Handhabung in der Praxis erfolgt. Während die Netzbetreiber zum Teil einen Beschluss nach §§ 100g, 100h StPO dafür verlangen, sind die Polizei- und Justizbehörden der Ansicht, dass die §§ 161, 163 StPO i. V. m. § 113 TKG die einschlägige Rechtsgrundlage sei. Hierdurch und durch weitere Konflikte, beispielsweise über Eilanordnungen, entstehen Reibungsverluste, insbesondere in Form von Verzögerungen. Dem entspricht es, wenn sich aus der Befragung deutliche Wahrnehmungen mangelnder Kooperationsbereitschaft seitens der Unternehmen ergeben. Probleme ergeben sich nach Angaben der Praktiker aus Polizei und Justiz auch daraus, dass die Netzbetreiber die Daten unterschiedlich lang speichern. Von den schriftlich befragten Staatsanwälten wurde überwiegend eine Speicherdauer von sechs bis zu zwölf Monaten befürwortet. In den Akten spielten freilich die Probleme mit der Speicherung der Daten lediglich bei 63 Beschlüssen eine Rolle; das sind nicht mehr als etwa 2 Prozent aller untersuchten Fälle. Bei 37 Beschlüssen waren die Daten bereits gelöscht und bei 17 Beschlüssen nur teilanonymisiert gespeichert. Offensichtlich hat sich die Strafverfolgungspraxis auf die Speicherungspraktiken der Unternehmen eingestellt. Ferner sind Verschlüsselungstechniken – jedenfalls als besonderes Problem – in den Akten nicht dokumentiert und werden als solches auch in den Befragungen und Interviews nur von einer Minderheit überhaupt thematisiert. Aber auch diese Personengruppe kann selbst dann, wenn tatsächlich Verschlüsselungstechniken zur Anwendung kamen, zumeist keine schwerwiegenden Auswirkungen auf den Ermittlungserfolg als Ganzes benennen, selbst wenn im Einzelfall ein Beschuldigter zunächst unidentifiziert blieb. Aus der Sicht von Telekommunikationsanbietern betreffen Probleme insbesondere fehlende Eindeutigkeit und Begrenzung der Beschlüsse. Während die Anbieter sich teilweise zur Überprüfung der Anfragen auch in materieller Hinsicht verpflichtet sehen, wird ihnen dieses Prüfungsrecht von den Polizei- und Justizbehörden abgesprochen. Die Anbieter sehen sich freilich in einem ständigen Konflikt zwischen der Umsetzung der Beschlüsse und dem Schutz der Rechte ihrer Kunden. Konflikte zwischen Unternehmen und Strafverfolgungsbehörden können, wenn auch selten, eskalieren, in Form von Hinweisen auf Zwangsmittel und die Einleitung von Verfahren wegen Strafvereitelung. Von den Unternehmen wird eine Zentralisierung der Abfragen in den Strafverfolgungsbehörden als eine erfolgversprechende Strategie in der Lösung von Implementationsproblemen gesehen. Ferner wird nach besserer Schulung und Spezialisierung verlangt.

XI. Kosten

Hinsichtlich der Kosten der Verkehrsdatenabfragen ist zu differenzieren zwischen Kosten, die die Einrichtung und die Unterhaltung der für die Überwachung notwendigen Organisation, Manpower, Hard- und Software betreffen und den Kosten, die für die einzelne Abfrage anfallen. Die Abfragekosten selbst scheinen über die durchschnittlichen Probleme hinaus keine Konfliktanlässe zu bieten. Die Infrastruktur- und Unterhaltungskosten stellen freilich, aus der Sicht der Unternehmen, ein ungelöstes Problem dar. Zunehmende Relevanz wird mit Einführung der Vorratsdatenspeicherung ferner die Sicherheit dieser Datenbestände erlangen. Neue Missbrauchsgefahren können hier technisch bedingt durch die Einrichtigung zusätzlicher Schnittstellen entstehen, und zwar sowohl im Hinblick auf Missbrauch von innen als auch im Hinblick auf unberechtigten Zugriff von außen. Die Forschungslage zu diesen Kosten zeigt freilich, dass bislang überzeugende Kostenanalysen nicht vorliegen.

F. Empfehlungen

I. Materielle Voraussetzungen und Klarstellungen im Gesetz

Die Anknüpfung der Verkehrsdatenabfrage an den Begriff der Straftat von erheblicher Bedeutung bei Verweis auf den Katalog des §100a StPO und die Tatbegehung durch Endgeräte führt offensichtlich dazu, dass unter das Merkmal der erheblichen Straftat auch Straftaten fallen, die allenfalls dem mittelschweren Kriminalitätsspektrum zuzuordnen sind. Dies ist offensichtlich dadurch bedingt, dass Veränderungen in der Tatphänomenologie spezifische Beweislagen mit sich bringen, in denen (ebenso wie bei Straftatbegehung durch Endgeräte) die Verkehrsdaten den einzig sinnvollen Ansatz für Ermittlungen bieten. Mit der Erweiterung der erheblichen Bedeutung um den Nachweis auch für den Einzelfall (§100g I Nr. 1 StPO) folgte die Reform (Bundesgesetzblatt 2007. I, Nr. 70, S. 3198) einerseits einer berechtigten Forderung, nämlich der materiellen Voraussetzung Flexibilität und Dehnbarkeit nach unten zu entziehen; andererseits dürfte sich damit der schon heute sichtbare Konflikt zwischen Nutzung und Ausschöpfung von Ermittlungsansätzen und dem Schutz von Freiheitsrechten verstärken. Plausibel scheint, die Voraussetzung der Tatbegehung durch Endgeräte zu ergänzen um eine **weitere Fallgruppe**, nämlich solchen (auch leichten) Straftaten (Diebstahl von Mobiltelefonen etc.), bei denen offensichtlich der Weg über die Verkehrsdaten der einzige Ermittlungsansatz ist.

Sowohl die Ergebnisse der Befragungen als auch die der Aktenanalyse zeigen, dass die Abfrage von Personendaten zu **dynamischen IP-Adressen** in der Praxis im Untersuchungszeitraum uneinheitlich gehandhabt wird. Mit §113 b Satz 1, Halbsatz 2 TKG wurde nunmehr eine Norm geschaffen, die jedenfalls auf einfachgesetzlicher Grundlage die Auskunft über Bestandsdaten erlaubt, auch wenn dabei auf Verkehrsdaten zurückgegriffen werden muss.

Wird eine Eilanordnung richterlich nicht bestätigt, so folgte nach dem Regierungsentwurf ein Beweisverwertungsverbot für personenbezogene Daten, sofern nicht Gefahr im Verzug bestand (§ 100b I StPO-E). Dies wurde aber in der zum 1. Januar 2008 in Kraft getretenen Fassung (§100b Abs. 1 Nr. 1 StPO) nicht übernommen. Insoweit wird das bestehende Konfliktpotential nicht beseitigt. Das Verwertungsverbot hätte ferner kaum Auswirkungen haben können, weil die eigentlichen Wirkungen übermittelter Daten im Ermittlungsverfahren selbst liegen und sich darin auch erschöpfen.

II. Formelle Voraussetzungen

Eine wirksame Implementation des **Richtervorbehalts** wird auch für die Verkehrsdatenabfrage mit den personellen Ressourcen bei Ermittlungsrichtern verbunden bleiben.

Die in §§100g II, Satz 1 in Verbindung mit §100b II StPO vorgesehene **Befristung** auf drei Monate sowie Verlängerungsmöglichkeiten von jeweils drei Monaten dürften die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, vollständig abdecken.

III. Organisation und Abläufe

Konfliktpotential entsteht nicht allein durch unterschiedliche Rechtsaufassungen, sondern auch dadurch, dass **wenig Standardisierung** zu beobachten ist. Hier stehen sich typisches Justizhandeln und das auf effiziente Abläufe ausgerichtete Unternehmensmodell gegenüber. Die **Konzentration** auf Schwerpunktabteilungen in der Strafverfolgung wäre überlegenswert.

Verbesserungen wären sicher auch möglich – wenngleich durch die föderale Struktur in Deutschland nur schwierig umsetzbar – durch die Entwicklung eines **Code of Practice,** der dem englischen Modell folgend gerade die organisatorischen und praktischen Elemente einer effizienten Verkehrsdatenabfrage enthält.

Nach der am 1. Januar in Kraft getretenen Reform ist die Benachrichtigungspflicht in § 101 VI ff. StPO geregelt. Dabei ist festgelegt, dass Personen zu benachrichtigen sind, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Dadurch wird klargestellt, dass die unbekannten Inhaber von Rufnummern nicht erst identifiziert und dadurch Grundrechtseingriffe noch verstärkt werden sollen, nur um die Benachrichtigungspflicht zu erfüllen. Hierfür bestand ebenso wie für die Dokumentationspflicht nach den Ergebnissen der Untersuchung Bedarf.

Dasselbe gilt für die Regelungen zu den Löschungspflichten.

IV. Statistik und Evaluation

Die Verpflichtung zur statistischen Erfassung der Anordnungen, zugrunde liegender Anlassstraftaten, Dauer der Maßnahme sowie ergebnisloser Maßnahmen, die nunmehr in § 100g IV StPO enthalten ist, entspricht der Europäischen Richtlinie und ist dazu geeignet Grunddaten zur Beschreibung der Anwendung zu erzeugen.

Die Erkenntnismöglichkeiten würden sich erweitern, wenn bereits an die Erhebung von Daten zu **beantragten** Anordnungen angeknüpft würde.

Ferner könnten die Kosten (ähnlich australischen und nordamerikanischen Erfassungen) aufgenommen werden.

V. Speicherungsdauer Verkehrsdaten

Die Festlegung einer Speicherungsfrist von sechs Monaten und damit am Minimum der EU-Richtlinie ist nach den sekundaranalytischen Feststellungen und den Ergebnissen der empirischen Untersuchung begründet. Aus der Studie lassen sich keine Hinweise entnehmen, dass eine darüber hinausgehende Speicherung die Aufklärungs-

quote bedeutsam erhöhen würde. Zwar werden aus der Befragung von Staatsanwälten Interessen an einer Speicherungsdauer von bis zu zwölf Monaten sichtbar. Doch weist die Aktenanalyse selbst unter den heutigen rechtlichen Bedingungen nur für etwa 2 Prozent der Abfragen nach, dass sie wegen Löschungen ins Leere gehen.

VI. Prüfungsrecht

Einige Telekommunikationsunternehmen reklamieren bislang offenbar eine Art „materielles Prüfungsrecht“ hinsichtlich der eingehenden Auskunftsanordnungen. Hier scheint aus Sicht dieser Unternehmen eine gewisse Unklarheit zu bestehen. Einerseits obliegt ihnen aus dem TKG die Sorgfaltspflicht bezüglich des Schutzes der anfallenden Kundendaten. Hierunter ist sicherlich eine formale Überprüfung der Richtigkeit der eingehenden Beschlüsse einschließlich der Personenidentität und Anschlussdaten (Rufnummern, IP-Adressen, etc.) zu fassen. Unzutreffend wäre jedoch, ebenso unstreitig, die Einräumung einer materiellen Kompetenz hinsichtlich richterlicher Beschlüsse. Nicht ganz so eindeutig verhält es sich freilich, wenn ein Eilantrag innerhalb der gesetzlichen Frist keine richterliche Bestätigung erhält. Für diese Fälle wäre eine gesetzliche Klarstellung erwägenswert.

VII. Entschädigung

Über die Kostenerstattung im Einzelfall hinaus ist an die Teilung der Kosten für Entwicklung und Unterhaltung der Überwachungs- und Kooperationssysteme zwischen Staat und Unternehmen zu denken. Hier könnte sich eine allgemeine, gegebenenfalls vom Einzelfall losgelöste Entschädigungsregelung im Rahmen des TKG empfehlen, um die in der Literatur vorherrschenden Bedenken[469] gegen die zunehmende Inanspruchnahme der Telekommunikationsanbieter im Rahmen der Telekommunikationsüberwachung dauerhaft entkräften.

[469] Bekanntlich ist gegenwärtig eine Verfassungsbeschwerde des VATM u. a. gegen die derzeitige Entschädigungsregelung im Zusammenhang mit der Auslandskopfüberwachung anhängig. Siehe für weitere Einzelheiten *Kilchling* 2008.

Literaturverzeichnis

Albers, Marion, Die verfassungsrechtliche Bedeutung der Evaluierung neuer Gesetze zum Schutz der Inneren Sicherheit, in: Menschenrechte – Innere Sicherheit – Rechtsstaat, Konferenz des Deutschen Instituts für Menschenrechte in Berlin am 27.6.2005. Berlin 2006, S. 21–36.

Albrecht, Hans-Jörg, Rechtstatsachenforschung zum Strafverfahren – empirische Untersuchungen zu Fragestellungen des Strafverfahrens zwischen 1990 und 2003, Neuwied, 2005.

Albrecht, Hans-Jörg, Organisierte Kriminalität: Zur sozialen Konstruktion einer Gefahr. Ein Kommentar, in: Organisierte Kriminalität – oder gesellschaftliche Desorganisation?, Angewandte Sozialforschung 22(2002), S. 155–160.

Albrecht, Hans-Jörg/Dorsch, Claudia/Krüpe, Christiane, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg i. Br., 2003.

Albrecht, Peter-Alexis, Die neu verfasste Polizei: Grenzverwischung und Geheimverfahren, Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft, Sonderheft, Winfried Hassemer zum 60. Geburtstag, Baden-Baden 2000, S. 17–24.

All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, London, Januar 2003.

Anechiarico, Frank/Jacobs, James, The Pursuit of Absolute Integrity, Chicago, London, 1996.

Arquilla, John/Ronfeldt, David (Hrsg.), Networks and Netwars: The Future of Terror, Crime, and Militancy, Washington: Rand 2001.

Artkämper, Heiko, Ermittlungsmaßnahmen in Funktelefonnetzen, Kriminalistik 1998, S. 202–207.

Ashworth, Andrew, Human Rights, Serious Crime and Criminal Procedure, London, 2002.

Australian Privacy Foundation submission to ACMA, Identity checks for pre-paid mobile phones, http://www.acma.gov.au/acmainterwr/_assets/main/lib100285/id_ checks_prepaid.pdf, Discussion Paper, April 2006.

Backes, Otto/Gusy, Christoph, Wer kontrolliert die Telefonüberwachung?, Frankfurt am Main, 2003.

Backes, Otto/Gusy, Christoph, Wer kontrolliert die Telefonüberwachung?, StV 2003, S. 249–252.

Backes, Otto/Lindemann, Michael, Staatlich organisierte Anonymität als Ermittlungsmethode bei Korruptions- und Wirtschaftsdelikten, Heidelberg, 2006.

Ball, Kirstie/Murakami Wood, David, A Report on the Surveillance Society, Wilmslow, 2006.

Bär, Wolfgang, Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100g, 100h StPO, MMR 2002, S. 358–364.

BDI-Positionspapier, „Telekommunikationsüberwachung verfassungsgemäß und wirtschaftsfreundlich gestalten“ vom 7.10.2003, S. 2, abrufbar unter http:/www.bdi-online.de.

Beck’scher TKG-Kommentar siehe Geppert (Hrsg.).

Berekoven, Ludwig/Eckert, Werner/Ellenrieder, Peter, Marktforschung: methodische Grundlagen und praktische Anwendung, 5. Auflage, Wiesbaden, 1991.

Beulke, Werner, Überwachung des Fernmeldeanschlusses eines Verteidigers, Jura 1986, S. 642–649.

Bignami, Francesca, Protecting Privacy Against the Police in the European Union: The Data retention Directive, Chicago Journal of International Law, 1/2007 (im Erscheinen).

Bizer, Johann, Die Evaluierung der Telekommunikations-Überwachung – Kritische Anmerkungen zur MPI-Studie, KrimJ 2003, S. 280–295.

Bizer, Johann/Günther, Oliver/Spiekermann, Sarah., Technikfolgenabschätzung – Ubiquitäres Computing und Informationelle Selbstbestimmung, Bundesministerium für Bildung und Forschung, Berlin, 2006.

BKA (Hrsg.), Informations- und Kommunikationskriminalität, Neuwied, 2004.

BKA (Hrsg.), Symposium: Der polizeiliche Erfolg, Wiesbaden, 1988.

Blum, Peter, Wege zu besserer Gesetzgebung – sachverständige Beratung, Begründung, Folgeabschätzung und Wirkungskontrolle, Gutachten I zum 65. Deutschen Juristentag, München, 2004.

Bradbury, Danny, No place to hide, Digital Investigation 2(2005), S. 244–246.

Bremer Institut für Kriminalpolitik (Hrsg.), Experimente im Strafrecht, Wie genau können Erfolgskontrollen von kriminalpräventiven Maßnahmen sein?, Bremen, 2000.

Brenner, Susan, Distributed Security: Moving Away From Reactive Law Enforcement, International Journal of Communications Law & Policy 9(2004), S. 1–43.

Breyer, Patrick, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin, 2005.

Breyer, Patrick, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal 11(2005), S. 365–375.

Brockhaus-Enzyklopädie, 19. Auflage, Band 6, Mannheim, 1988.

Brüning, Janique, Der Richtervorbehalt im strafrechtlichen Ermittlungsverfahren, Baden-Baden, 2005.

Büchler, Heinz/Wagner, Dieter/Grawert, Achim/Fiedler, Anne-Kathrin, Effektivität und Effizienz kriminalpolizeilicher Organisationsformen auf Zeit, Wiesbaden, 1994.

Büllingen Franz/Gillet, Aurélia/Gries, Christin-Isabel/Hillebrand, Annette/Stamm Peter, Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich, wik-Consult, Bad Honnef, Oktober 2004.

Büllingen, Franz, Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich, DuD 2005, S. 349–353.

Bundesinnenministerium, Fakten zur Evaluierung des Terrorismusbekämpfungsgesetzes, Berlin, 11. Mai 2005.

Bundesnetzagentur, Jahresbericht, 2006.

Caprioli, Eric/Saadoun, Ygal/Cantero, Isabelle, The Right to Digital Privacy: A European Survey, Rutgers Journal of Law & Urban Policy 3(2006), S. 211–218.

Centre for Policy Research on Science and Technology, Privacy Rights and Prepaid Communication Services, A survey of prepaid mobile phone regulation and registration policies among OECD member states, Simon Fraser University, Vancouver, 2006.

Council of Europe, Terrorism: special investigation techniques, Strasbourg, 2005.

Covington&Burling, Memorandum of Laws Concerning the Legality of Data Retention with Regard to the Rights Guaranteed by the European Convention on Human Rights, Prepared for Privacy International, 10th October 2003.

Crump, Catherine, Data Retention: Privacy, Anonymity, and Accountability Online, Stanford Law Review 56(2003), S. 191–229.

Cyber Security Industry Alliance, Data Retention: Get the Facts, Arlington, 2007.

Danckwerts, Rolf Nikolas, Funkzellenabfrage gemäß § 100h I Satz 2 StPO, CR 7/2002, S. 539–543.

Danezis, George/Wittneben, Bettina, The Economics of Mass Surveillance and the Questionable Value of Anonymous Communications, K. U. Leuven, ESAT/COSIC, RSM Erasmus University Rotterdam, 2006.

Deckers, Rüdiger, Geheime Aufklärung durch Einsatz technischer Mittel, StraFo 2002, S. 109–118.

Demko, Daniela, Die Erstellung von Bewegungsbildern mittels Mobiltelefon als neuartige strafprozessuale Observationsmaßnahme, NStZ 2004, S. 57–64.

Deutscher Richterbund (Hrsg.), Handbuch der Justiz, Heidelberg, 2004.

Dix, Alexander, Informations- und Kommunikationskriminalität, Kriminalistik 2004, S. 81–85.

Dorsch, Claudia, Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, Berlin, 2005.

Dreier, Horst, Grundgesetz, Kommentar, 2. Auflage, Tübingen, 2004.

Eagle, Nathan/Pentland, Alex/Lazer, David, Inferring Social Network Structure using Mobile Phone Data, Proceedings of the National Academy of Sciences 2007 (in submission).

Eckhardt, Jens, Telekommunikations-Überwachungsverordnung – Ein Überblick, CR 10/2001, S. 670–678.

Esser, Robert, Auf dem Weg zu einem europäischen Strafverfahrensrecht, Berlin, 2002.

Etzioni, Amitai, The Spirit of the Community: Rights, Responsibilities and the Communitarian Agenda, London 1995.

European Working Party on Information Technology Crime, Expert Statement, Overview of vital traffic data necessary for investigations for which the EWPITC asks the general retention by telecommunication operators and telecommunication access and service providers, Interpol, 26. 11. 2001.

Faculteit der Rechtsgeleerdheid, Erasmus Universiteit Rotterdam: Wie wat bewaart die heeft wat. Onderzoek naar nut en noodzaak van een bewaarverplichting voor historische verkeersgegevens van telekommunicatieverkeer, Rotterdam, 2005.

Farmer, Dan/Mann, Charles, Surveillance Nation, Technology Review 2004, S. 1–10.

Figliola, Patricia, Digital Surveillance: The Communications Assistance for Law Enforcement Act CRS Report for Congress, Washington 2007.

Fijnaut, Cyrille/Paoli, Letitia (Hrsg.), Organised Crime in Europe, Concepts, Patterns and Control Policies in the European Union and Beyond, Dordrecht, 2004.

François, Jean-Marc, Performing and Making Use of Mobility Prediction, Universität Liège, 2007.

Friedrich, Dirk, Die Verpflichtung privater Telekommunikationsunternehmen, die staatliche Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, Aachen, 2001.

Geppert, Martin (Hrsg.), Beck´scher TKG-Kommentar, 3. Auflage, München, 2006.

Gercke, Björn, Überwachung des Mobilfunkverkehrs – Das Handy als „Allroundmittel“ zur Ausforschung, Bürgerrechte & Polizei/CILIP 71(2002), S. 20–28.

Geser, Hans, Towards a Sociological Theory of the Mobile Phone, http://socio.ch/mobile/t_geser1.pdf, 2004.

Gilbert, Daphne/Kerr, Ian R./McGill, Jena, The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers, Criminal Law Quarterly 51(2007), S. 469–507.

Gnirck, Karen/Lichtenberg, Jan, Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen, DuD 2004, S. 598–602.

Goemans, Caroline/Dumortier, Jos, Enforcement Issues – Mandatory retention of traffic data in the EU: possible impact on privacy and on-line anonymity, Interdisciplinary Centre for Law and Information, Faculty of Law, K. U. Leuven 2003.

Gow, Gordon A., Privacy Rights and Prepaid Communications Services: A Survey of

Prepaid Mobile Phone Regulation and Registration Policies among OECD Member States, Research report for the Office of the Privacy Commissioner of Canada, Prepared by the Centre for Policy Research on Science and Technology, Simon Fraser University at Harbour Centre, Vancouver, Canada, March 31, 2006.

Gow, Gordon A./Ihnat, Mark, Prepaid Mobile Phone Service and the Anonymous Caller: Considering Wireless E9-1-1 in Canada, Surveillance & Society 1(2004), S. 555–572.

Günther, Ralf, Spannungsfeld: Strafverfolgung und Service-Provider, Kriminalistik 2004, 11–16.

Gusy, Christoph, Das Fernmeldegeheimnis von Pressemitarbeitern als Grenze strafprozessualer Ermittlungen, NStZ 2003, S. 399–403.

Hammerstein, Christian von, Kostentragung für staatliche Überwachungsmaßnahmen nach der TKG-Novelle, MMR 2004, S. 222–227.

Herz, Annette Louise, Menschenhandel – eine empirische Untersuchung zur Strafverfolgungspraxis, Freiburg i. Br., 2006.

Hess, Henner, Jenseits von Huxley und Orwell, Alte und neue Prognosen über die Zukunft der Kontrollpolitik, in: Althoff, M. et al: Integration und Ausschließung, Kriminalpolitik und Kriminalität in Zeiten gesellschaftlicher Transformation, Baden-Baden, 2001, S. 322–341.

Hoeren, Thomas, Auskunftspflichten der Internetprovider an Strafverfolgungs- und Sicherheitsbehörden – eine Einführung, wistra 2005, S. 1–9.

Hoeren, Thomas, Recht der Access Provider, München, 2004.

Holznagel, Bernd/Enaux, Christoph/Nienhaus, Christian, Telekommunikationsrecht, 2. Auflage, München, 2006.

Karlsruher Kommentar siehe Pfeiffer (Hrsg.).

Keller, Christoph, Die Standortbestimmung von Mobiltelefonen, Die Polizei 2005, S. 106–114.

Kilchling, Michael, Die Neuregelung zur Auslandskopfüberwachung gemäß § 4 TKÜV auf dem verfassungsrechtlichen Prüfstand, Freiburg i. Br., 2008 (im Erscheinen).

Kinzig, Jörg, Die rechtliche Bewältigung von Erscheinungsformen organisierter Kriminalität, Berlin, 2004.

Kinzig, Jörg, Die Telefonüberwachung in Verfahren organisierter Kriminalität: Fehler bei der richterlichen Anordnung, Mängel des Gesetzes, StV 2004, S. 560–567.

Köbele, Bernd, Anspruch auf Mitteilung des Anschlussinhabers bei bekannter IP-Adresse, DuD 2004, S. 609–610.

KPMG Informatie Risk Management, Onderzoek naar de opslag van historische verkeersgegevens van telecommunicatieaanbieders, Amstelveen, November 2004.

Kube, Hanno/Schütze, Marc, Die Kosten der TK-Überwachung, CR 2003, S. 663–671.

Kunert, Karl H., Erweitertes Zeugnisverweigerungsrecht der Medienmitarbeiter – Gesetz zur Änderung der Strafprozessordnung vom 15. 2. 2002, NStZ 2002, S. 169–174.

Kürzinger, Josef, Private Strafanzeige und polizeiliche Reaktion, Berlin, 1978.

Laasonen, Kari, Route Prediction from Cellular Data, Basic Research Unit, Helsinki Institute for Information Technology, Department of Computer Science, University of Helsinki, 2006.

Langheinrich, Marc, Gibt es in einer total informatisierten Welt noch eine Privatsphäre?, in: Mattern, Friedemann (Hrsg), Die Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin, 2007, S. 232–264.

Larnhof, Karin, Data Retention – Zur aktuellen Rechtslage in einigen EU-Mitgliedsländern unter Berücksichtigung der EU-Richtlinie zur Vorratsdatenspeicherung, Eisenstadt, 2006.

Ledergerber, Zora, Whistleblowing unter dem Aspekt der Korruptionsbekämpfung, Bern, 2005.

Leibholz, Gerhard/Rinck, Hans J., Grundgesetz für die Bundesrepublik Deutschland, Kommentar an Hand der Rechtsprechung des BVerfG, Köln, 46. Lieferung, Juli 2007.

Löwe, Ewald/Rosenberg, Werner, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 25. Auflage, Berlin, 2004.

Lüken, Wiard, Auskunft über Telekommunikationsverbindungsdaten – §§ 100g, 100h StPO, Die Polizei 2002, S. 224–225.

Mahnken, Eva, Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten, Rechtstatsachen zum Beleg der defizitären Rechtslage, Wiesbaden, November 2005.

Marx, Gary T., Seeing Hazily (But Not Darkly) Through the Lens: Some Recent Empirical Studies of Surveillance Technologies, Law & Social Inquiry 2006, S. 339–399.

Marx, Gary T., Undercover Police Surveillance in America, Berkely, Los Angeles, London, 1988.

Maunz, Theodor/Dürig, Günter, Grundgesetz, Band II (Artikel 6 – 16a), München, 47. Lieferung, Juni 2006.

Mayer, Horst, Interview und schriftliche Befragung, 3. Auflage, München/Wien, 2006.

Meyer-Goßner, Lutz, Strafprozessordnung, 49. Auflage, München, 2006.

Meyer-Wieck, Hannes, Der Große Lauschangriff – eine empirische Untersuchung zu Anwendung und Folgen § 100c I Nr. 3 StPO, Berlin, 2005.

Mountain, David M., Exploring mobile trajectories: An investigation of individual spatial behaviour and geographic filters for information retrieval, City University, Department of Information Science, London, 2005.

Nevis Consulting Group Inc., Summary of Submissions to the Lawful Access Consultation, Ottawa, 2003.

Nuno Alvaro, Alexander, Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, Europäisches Parlament, Arbeitsdokument vom 21.1.2005.

OECD, Communications Outlook 2007, Paris, 2007.

Office of the Inspector General, The Implementation of the Communications Assistance for Law Enforcement Act Audit Report 06-13, March 2006.

Ortmann, Rüdiger, Sozialtherapie im Strafvollzug – Eine experimentelle Längsschnittstudie zu den Wirkungen von Strafvollzugsmaßnahmen auf Legal- und Sozialbewährung, Freiburg i. Br., 2002

Pehl, Dirk, Die Implementation der Rasterfahndung – Eine empirische Untersuchung zur Wirkmächtigkeit der gesetzlichen Regelungen zur operativen Informationserhebung durch Rasterfahndung, Freiburg i.Br., 2008 (im Erscheinen).

Peissl, Walter, Surveillance and Security: A Dodgy Relationship. Journal of Contingencies and Crisis Management 11(2003), S. 19–24.

Petersen, Rodney, Toward a U.S. Data Retention Standard for ISPs, EDUCAUSE Review 2006, S. 78–79.

Pfeiffer, Gerd (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz, 5. Auflage, München, 2003.

Pfeiffer, Gerd, Strafprozessordnung, 5. Auflage, München, 2005.

Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen, Modernisierung des Datenschutzrechts. Bundesministerium des Inneren, Berlin, 2001.

Rowland, Diane, Data Retention and the War Against Terrorism – A Considered and Proportionate Response?, The Journal of Information, Law and Technology (JILT) 2004 (3).

Rudolphi, Hans-Joachim, Systematischer Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz, Frankfurt am Main, 50. Lfg., Stand: Oktober 2006.

Sachs, Michael (Hrsg.), Grundgesetz, 2. Auflage, München, 1999.

Sankol, Barry, Die Qual der Wahl: § 113 TKG oder §§ 100g, 100h StPO? – Die Kontroverse über das Auskunftsverlangen von Ermittlungsbehörden gegen Access-Provider bei dynamischen IP-Adressen, MMR 2006, S. 361–365.

Sankol, Barry, Strafprozessuale Zwangsmaßnahmen und Telekommunikation – Der Regelungsgehalt der §§ 100a ff. StPO, JuS 2006, S. 698–703.

Schaar, Peter, Mit heißer Nadel gegen den Terrorismus?, MMR 2001, S. 713–714.

Schmidt, Volker, Telekommunikations (TK) – Verbindungsdaten, Der Kriminalist 5/2002, S. 210–214.

Schmidt-Preuß, Matthias, Kurzgutachten „Die verfassungsrechtlichen Anforderungen an die Entschädigung für Leistungen der Telekommunikationsüberwachung und der Auskunftserteilung“, Bonn, 4. Mai 2005.

Schramm, Marc, Staatsanwaltschaftliche Auskunft über dynamische IP-Adressen, DuD 2006, S. 785–788.

Schulzki-Haddouti, Christiane, Sicherheit im Netz und digitale Bürgerrechte, Aus Politik und Zeitgeschichte 50 (2003), S. 13–19.

Seitz, Nicolai, Strafverfolgungsmaßnahmen im Internet, Köln, 2004.

Sierck, Gabriela M./Schöning, Frank/Pöhl, Matthias, Wissenschaftliche Dienste des Deutschen Bundestages, Gutachten zur „Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht“, 2006.

Sofsky, Wolfgang, Verteidigung des Privaten, München, 2007.

Statistisches Bundesamt (Hrsg.), Rechtspflege, Fachserie 10/ Reihe 2.6: Staatsanwaltschaften 2003, Wiesbaden, 2004.

Steffen, Wiebke, Analyse polizeilicher Ermittlungstätigkeit aus der Sicht des späteren Strafverfahrens, Wiesbaden, 1976.

Steinhardt, Barry, Trend Report – Does Privacy Have a Future after 9/11?, Journal of Contingencies and Crisis Management 11(2003), S. 32–36.

Systematischer Kommentar zur StPO siehe Rudolphi.

Taipale, Kim, Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance, New York University Review of Law and Security 7(2006), S. 1–6.

Tak, Peter, J. P., Heimelijke Opsproing in de Europese Unie, Antwerpen, Groningen 2000.

The Surveillance Project, Global Privacy of Data, International Survey, Queens University Belfast, 2006.

Volkmar, Rolf-Dieter, Kriminalistische Akustik und Telefonüberwachung (TÜ), Der Kriminalist (30), 1997, S. 191–206.

Waechter, Kay, Bereitstellungspflichten für Fernmeldeanlagenbetreiber, VerwA 1996, S. 68–96.

Walker, Clive/Akdeniz, Yaman, Anti-Terrorism Laws and Data Retention: War is Over?, Northern Ireland Legal Quarterly 54(2003), S. 159–182.

Warner, Jeremy, The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps, University of Ottawa Law & Technology Journal 2(2005), S. 75–104.

Weinzierl, Ruth, Die Evaluierung von Sicherheitsgesetzen, Anregungen aus menschenrechtlicher Perspektive, Berlin, 2006.

Welp, Jürgen, Überwachung und Kontrolle, Berlin, 2000.

Welp, Jürgen, Verbindungsdaten – Zur Reform des Auskunftsrechts (§§ 100g, 100h StPO), GA 2002, S. 535–556.

Weßlau, Edda, Anm. zu BGH 1 StR 685/95 (LG Konstanz) vom 23.3.1996 «Prüfungsumfang bei Zustimmung zum Einsatz eines VE», StV 11 (1996), S. 579–580.

Weßlau, Edda, Gefährdungen des Datenschutzes durch den Einsatz neuer Medien im Strafprozess, ZStW 113 (2001), S. 681–708.

Wohlers, Wolfgang/Demko, Daniela, Der strafprozessuale Zugriff auf Verbindungsdaten (§§ 100g, 100h StPO), StV 2003, S. 241–248.

Wolff, Reinmar/Neumann, Andreas, Anordnung der Auskunft über Telekommunikationsverbindungsdaten gegen unbekannt?, NStZ 2003, S. 404–408.

Wollweber, Harald, Verbindungsdaten der Telekommunikation im Visier der Strafverfolgungsbehörden, NJW 2002, S. 1554–1556.

Wolter, Jürgen, Aspekte einer Strafprozessreform bis 2007, München 1991.

Wolter, Jürgen/Schenke, Wolf-Rüdiger, Zeugnisverweigerungsrechte bei (verdeckten) Ermittlungsmaßnahmen, Berlin, 2002.

Wu, Jiuan-Yih, Strafprozessuale Telekommunikationsüberwachung in der Informationsgesellschaft, Frankfurt am Main, 2005.

Zimmermann, Peter, JVEG, Kommentar, Bielefeld, 2005.

Anhang

A. Fragebogen für die Aktenanalyse

Verfahren

v001 Fall_Nr. (*Bearbeiternr.2stellig;Anzahl bearbeiteter Akten 3stellig:z.B. 05025)*: ....

v002 AZ: ....

v003 Landgerichtsbezirk: ....

v004 Bundesland
1 Baden-Württemberg
2 Berlin
3 Nordrhein-Westfalen
4 Mecklenburg-Vorpommern

v005 Datum der Einleitung eines polizeilichen Ermittlungsverfahrens: ....

v006 Datum des polizeilichen Abschlussberichts/des Schlussvermerks: ....

v007 Inhalt Polizeilicher Abschlussbericht
1 Tat(en) gelten als aufgeklärt
2 Ermittlungen werden erfolglos eingestellt
0 Sonstiges: ....

v008 Worauf wird das Ermittlungsergebnis im Abschlussbericht gestützt? (*Mehrfachnennungen*)
1 TK-Daten
2 TÜ
3 Zeugenaussagen
4 Aussage V-Person
5 Aussage verdeckter Ermittler
6 Andere sachliche Beweismittel (*Augenschein, Urkunde, SV*)
0 Sonstiges: ....

v009 Werden TK-Daten im Abschlußbericht erwähnt?
1 ja
2 teilweise: ....
3 nein
0 Sonstiges: ....

v010 Ermittelnde Polizeibehörde (*Polizeilicher Abschlussbericht*)
1 Kripo
2 Schutzpolizei
3 LKA
4 BKA
5 BGS
6 GER (Gemeinsame Ermittlungsgruppe Rauschgift)
7 ZKA (Zollkriminalamt)
0 Sonstiges: ....

v011 Dezernat
1 OK/Bande
2 BtM
3 Wirtschaftskriminalität
4 Jugendsachen
5 Allgemeines Dezernat
0 Sonstiges:...................................

v012 Datum der ersten Einschaltung der StA: ....

v013 Grund der Einschaltung der StA
1 Allgemeine Anzeige
2 Anregung §§100gh-Maßnahme
3 Anregung TÜ
4 Anregung Haftbefehl
5 Anregung Durchsuchung
6 Anregung Verdeckter Ermittler
7 Anregung Wohnraumüberwachung
8 Anregung Beschlagnahme
9 Anregung andere technische Maßnahmen
0 Sonstiges:....................................

v014 Verfahren gegen Unbekannt
1 ja
2 nein
3 zunächst ja, später Beschuldigter bekannt

v015 Gegen wie viele Personen wird ermittelt: ....

v016 Anzahl der als Beschuldigte geführten Personen: ....

Tatphänomenologie

Politische Delikte (§ 100a Satz 1 Nr. 1a StPO)
v017 Welche Art: (*Schwerpunkt*)
1 Friedensverrat (§§ 80-80a StGB)
2 Hochverrat (§§ 81-82 StGB)
3 Gefährdung des demokratischen Rechtsstaats (§§ 84-86, 87-89 StGB)
4 Landesverrat (§§ 94 StGB)
5 Gefährdung der äußeren Sicherheit (§§ 95-100a StGB)
0 Sonstige: ....

v018 Politische Delikte: Gesamtgruppe?
1 ja
2 nein

Straftaten gegen die Landesverteidigung (§ 100a Satz 1 Nr. 1b StPO)
v019 Welche Art:
1 § 109d StGB
2 § 109e StGB
3 § 109f StGB
4 § 109g StGB
5 § 109h StGB

v020 Straftaten nach § 100a Satz 1 Nr. 1b StPO: Gesamtgruppe?
1 ja
2 nein

Vereinigungsdelikte (§ 100a Satz 1 Nr. 1c StPO)
v021 Welche Art:
1 Kriminelle Vereinigung (§ 129 StGB)
2 Terroristische Vereinigung (§ 129a StGB)
3 Kriminelle und terroristische Vereinigungen im Ausland (§ 129b StGB)
4 Volksverhetzung (§ 130 StGB)
5 § 95 Abs. 1 Nr. 8 AufenthG (Geheime Vereinigung)
0 Sonstige: ....

v022 Gruppenbezeichnung: ....
v023 Anzahl der Personen der Vereinigung: ....

v024 Kurze Schilderung des Sachverhalts (Stichworte): ....
....

v025 Vereinigungsdelikte: Gesamtgruppe?
1 ja
2 nein

Anstiftung und Beihilfe zur Fahnenflucht oder Anstiftung zum Ungehorsam (§ 100a Satz 1 Nr. 1d StPO)

v026 Welche Art:
1 Anstiftung zur Fahnenflucht
2 Beihilfe zur Fahnenflucht
3 Anstiftung zum Ungehorsam

v027 Delikte i.S.d. § 100a Satz 1 Nr. 1d StPO: Gesamtgruppe?
1 ja
2 nein

Straftaten i.S.d. § 100a Satz 1 Nr. 1e StPO

v028 Wenn Straftat i.S.d. § 100a Satz 1 Nr. 1e StPO, welche Art: ....

v029 Delikte i.S.d. § 100a Satz 1 Nr. 1e StPO: Gesamtgruppe?
1 ja
2 nein

Fälschungsdelikte

v030 Welches Delikt:
1 Geldfälschung (§ 146 StGB)
2 Wertpapierfälschung (§ 151 StGB)
3 Geld-/Wertpapierfälschung bei fremdem Währungsgebiet (§ 152 StGB)
0 Sonstige: ....

v031 Währung: ....

v032 Wertpapiere (*Art*): ....

v033 Größenordnung/Wert (*in EUR*): ....

v034 Fälschungsdelikte: Gesamtgruppe?
1 ja
2 nein

Straftaten gegen die sexuelle Selbstbestimmung

v035 Welche Art:
1 Schwerer sexueller Missbrauch von Kindern (§ 176a Abs. 1-3, 5 StGB)
2 Sexueller Missbrauch von Kindern mit Todesfolge (§ 176b StGB)
3 Sexueller Missbrauch von Kindern (§ 176 StGB)
4 Vergewaltigung/Sexuelle Nötigung (§ 177 StGB)
5 Vergewaltigung/Sexuelle Nötigung mit Todesfolge (§ 178 StGB)
6 Sexueller Missbrauch von Jugendlichen (§ 182 StGB)
0 Sonstige: ....

v036 Anzahl der Opfer: ....

v037 Kam es zum Tod und/oder zur Körperverletzung eines Opfers?
1 Tod
2 leichte Körperverletzung
3 mittlere Körperverletzung
4 schwere Körperverletzung

v038 Täter-Opfer-Beziehungen:

1 Familie
2 Verwandtschaft
3 Freunde/Bekannte
4 Keine Beziehung

v039 Straftaten gegen die sexuelle Selbstbestimmung: Gesamtgruppe?
1 ja
2 nein

Verbreitung pornographischer Schriften

v040 Welche Art:
1 Verbreitung pornografischer Schriften
2 § 184b Abs.3 StGB (Verbr. p. Schriften als Mitglied einer Bande oder gewerbsmäßig)
0 Sonstige: ....

v041 Kurze Sachverhaltsschilderung (in Stichworten): ....
....

v042 Wenn mittels Endeinrichtung begangen, welche Art von Endeinrichtung: (*MN möglich*)
1 Telefon
2 Handy
3 Fax
4 Computer
0 Sonstige: ....

v043 Verbreitung pornographischer Schriften: Gesamtgruppe?
1 ja
2 nein

Tötungsdelikte

v044 Welche Art:
1 Mord
2 Totschlag
3 Völkermord
4 Tötung auf Verlangen
0 Sonstige: ....

v045 Anzahl der Opfer: ....

v046 Erscheinungsbild
1 Beziehungstat
2 Verdeckungstat
3 Raubmord
4 Sexualmord
0 Sonstige: ....

v047 Tötungsdelikte: Gesamtgruppe?
1 ja
2 nein

Straftaten gegen die persönliche Freiheit

v048 Welche Art:
1 Menschenhandel zum Zweck der sexuellen Ausbeutung (§ 232 StGB)
2 Spezialfall des § 232 Abs. 3, 4, 5 StGB
3 Menschenhandel zum Zweck der Ausbeutung der Arbeitskraft (§ 233 StGB)
4 Spezialfall des § 233 Abs. 3 StGB
5 Menschenraub (§ 234 StGB)
6 Verschleppung (§ 234a StGB)
7 Erpresserischer Menschenraub (§ 239a StGB)
8 Geiselnahme (§ 239b StGB)
9 Entziehung Minderjähriger (§ 235 StGB)

10 Kinderhandel (§ 236 StGB)
11 Freiheitsberaubung (§ 239 StGB)
12 Nötigung (§ 240 StGB)
13 Bedrohung (§ 241 StGB)
0 Sonstige: ....

v049 Wenn Bedrohung mittels Endeinrichtung begangen, mittels welcher Endeinrichtung:
1 Telefon
2 Handy
3 Fax
4 Computer
0 Sonstige:............................

v050 Größenordnung (*Anzahl der Personen*): ....

v051 Kam es zum Tod und/oder zur Körperverletzung von Personen?
1 Tod
2 leichte Körperverletzung
3 mittlere Körperverletzung
4 schwere Körperverletzung

v052 Straftaten gegen die persönliche Freiheit: Gesamtgruppe?
1 ja
2 nein

Diebstahl

v053 Welche Art:
1 Diebstahl (§ 242 StGB)
2 Besonders schwerer Fall des Diebstahls (§ 243 StGB)
3 Diebstahl mit Waffen (§ 244 I Nr. 1 StGB)
4 Bandendiebstahl (§ 244 I Nr. 2 StGB)
5 Wohnungseinbruchsdiebstahl (§ 244 I Nr. 3 StGB)
6 Schwerer Bandendiebstahl (§ 244a StGB)
0 Sonstige: ....

v054 Besonderes Erscheinungsbild:
1 Kfz-Diebstahl
2 Einbruchsdiebstahl
0 Sonstiges: ....

v055 Anzahl der angenommenen Delikte: ....

v056 Schadenshöhe (EUR): ....

v057 Wenn Opfer juristische Person:
1 Staat
2 Bank/Zahlstellen
3 Betriebe
4 Einzelhandelsgeschäfte
5 Versicherung

v058 Diebstahl: Gesamtgruppe?
1 ja
2 nein

Raub und (räuberische) Erpressung

v059 Welche Art:
1 Raub (§ 249 StGB)
2 Schwerer Raub (§ 250 StGB)
3 Raub mit Todesfolge (§ 251 StGB)
4 Räuberischer Diebstahl (§ 252 StGB)
5 Erpressung (§ 253 StGB)

6 Räuberische Erpressung (§ 255 StGB)

v060 Besonderes Erscheinungsbild
1 Bankraub
2 Sonstige Geschäfte
3 Wohnungsraub
4 Straßenraub
0 Sonstiges: ....

v061 Höhe des Schadens (*in EUR*): ....

v061a Wenn mittels Endeinrichtung begangen, welche Art von Endeinrichtung:
1 Telefon
2 Handy
3 Fax
4 Computer
0 sonstige:.............................

v062 Raub/Erpressung: Gesamtgruppe?
1 ja
2 nein

Hehlerei

v063 Welche Art:
1 Hehlerei (§ 259 StGB)
2 Gewerbsmäßige Hehlerei (§ 260 StGB)
3 Bandenhehlerei (§ 260 StGB)
4 Gewerbsmäßige Bandenhehlerei (§ 260a StGB)

v064 Größenordnung (*in EUR*): ....

v065 Hehlerei: Gesamtgruppe?
1 ja
2 nein

Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte

v066 Welche Art:
1 Geldwäsche
2 Verschleierung unrechtmäßig erlangter Vermögenswerte
3 Spezialfall des § 261 Abs. 1, 2 o. 4 StGB

v067 Größenordnung (*in EUR*): ....

v068 Geldwäsche/Verschleierung: Gesamtgruppe?
1 ja
2 nein

Gemeingefährliche Straftaten

v069 Welche Art:
1 Brandstiftung (§ 306 StGB)
2 Schwere Brandstiftung (§ 306a StGB)
3 Besonders schwere Brandstiftung (§ 306b StGB)
4 Brandstiftung mit Todesfolge (§ 306c StGB)
5 Vorsätzliches Herbeiführen einer Explosion durch Kernenergie, § 307 Abs. 1-3 StGB
6 Herbeiführen einer Sprengstoffexplosion (§ 308 StGB)
7 Missbrauch ionisierender Strahlen (§ 309 Abs.1-4 StGB)
8 Vorbereitung eines Explosions- oder Strahlungsverbrechens (§ 310 Abs. 1 StGB)
9 Herbeiführung einer Überschwemmung (§ 313 StGB)
10 Gemeingefährliche Vergiftung (§ 314 StGB)
11 Gefährl. Eingriff in den Bahn-, Schiffs- und Luftverkehr (§ 315 StGB)
12 Qualifikation § 315 Abs. 3 StGB

13 Gefährl. Eingriff in den Straßenverkehr (§ 315b StGB)
14 Qualifikation § 315b Abs. 3 StGB
15 Gefährdung des Straßenverkehrs (§ 315c StGB)
16 räuberischer Angriff auf Kraftfahrer (§ 316a StGB)
17 Angriffe auf den Luft- und Seeverkehr (§ 316c StGB)
0 Sonstige: ....

v070 Schadenshöhe (*in EUR):*..

v071 Anzahl der gefährdeten Personen: ....

v072 Möglicher Sachschaden: ....

v073 Kam es zum Tod und/oder zu Körperverletzungen von Personen
1 Tod
2 leichte Körperverletzung
3 mittlere Körperverletzung
4 schwere Körperverletzung

v074 Gemeingefährliche Straftaten: Gesamtgruppe?
1 ja
2 nein

Verstöße gegen das Waffengesetz

v075 Welche Art:
1 § 51 WaffG
2 § 52 WaffG
0 Sonstige: ....

v076 Größenordnung *(Anzahl/Bezeichnung*): ....

v077 Wert (*in EUR*): ....

v078 Waffen: Gesamtgruppe?
1 ja
2 nein

Verstöße gegen das Außenwirtschaftsgesetz

v079 Welche Art:
1 § 34 Abs. 1-6 AußenwirtG (i.V.m. KrWKG)
2 § 19 Abs. 1-3 AußenwirtG (i.V.m. KrWKG)
3 § 20 Abs. 1 oder 2 AußenwirtG (i.V.m. KrWKG)
0 Sonstige: ....

v080 Tatobjekt (*in Stichworten*): ....

v081 Außenwirtschaft: Gesamtgruppe?
1 ja
2 nein

Betäubungsmitteldelikte

v082 Welche Art:
1 § 29 BtMG
2 Spezialfall § 29 Abs. 3 Satz 2 Nr. 1 BtMG
3 § 29a BtMG
4 § 30 (Abs. 1 Nr. 1, 2, 4) BtMG
5 § 30a BtMG
6 § 30b BtMG
7 Sonstige: ....

v083 Wenn Betäubungsmitteldelikte: Art der Drogen?

1 Heroin
2 Kokain
3 Haschisch
4 Amphetamine
5 Ecstasy
0 Sonstiges: ....

v084 Menge (*in Gramm*): ....

v084a Menge (*Anzahl der Tabletten*): ....

v085 (Vermutete) Dauer des Handels/Vertriebs (*in Monaten*): ....

v086 Einordnung bei Handel/Vertrieb
1 Kleinverteiler (*Grammbereich und direkter Kontakt mit Konsumenten*)
2 Zwischenhandel
3 Großhandel (*ab Kilobereich*)

v087 Grenzüberschreitende Elemente
1 Typische Einkaufsfahrten
2 Feste Lieferanten im Ausland
3 Dauerhaft grenzüberschreitende Struktur
4 Nein

v088 BtM: Gesamtgruppe?
1 ja
2 nein

Verstöße gegen das Ausländerrecht

v089 Welche Art:
1 § 92a AuslG bzw. § 96 Abs. 2 AufenthG (Einschleusen von Ausländern)
2 § 92b AuslG bzw. § 97 AufenthG (gewerbs- u. bandenmäßiges Einschleusen)
3 andere §§ im AuslG bzw. AufenthG: ....
4 §§ 84 Abs. 3, 84a AsylVfG (gewerbs- o. bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung)
5 andere §§ im AsylVfG: ....
0 Sonstiges: ....

v090 Größenordnung (*Anzahl der Personen*): ....

v091 Ausländerrecht: Gesamtgruppe?
1 ja
2 nein

Betrug

v092 Welche Art:
1 Betrug (§ 263 StGB)
2 Besonders schwerer Fall des Betrugs (*welche Art*): ....
3 Computerbetrug (§ 263a StGB)
0 Sonstige

v093 Besonderes Erscheinungsbild
1 Bankbetrug
2 Wirtschaftsbetrug
3 Enkeltrick
4 Ebay-/Internetbetrug/Warenbestellbetrug
0 Sonstiges ......

v094 Höhe des Schadens (*in EUR*): ....

v095 Wenn mittels Endeinrichtung begangen, welche Art von Endeinrichtung:

1 Telefon
2 Handy
3 Fax
4 Computer
0 sonstige:............................

v096 Betrug: Gesamtgruppe?
1 ja
2 nein

Körperverletzungsdelikte

v097 Welches Delikt:
1 Körperverletzung (§ 223 StGB)
2 Gefährliche Körperverletzung (§ 224 StGB)
3 Schwere Körperverletzung (§ 226 StGB)
4 Körperverletzung mit Todesfolge (§ 227 StGB)
0 Sonstiges: ....

v098 Anzahl der Opfer: ....

v099 Verletzungsintensität
1 Leicht (*keine ärztliche Behandlung*)
2 Mittel (*ärztliche Behandlung*)
3 Schwer (*Krankenhaus*)

v100 Körperverletzung: Gesamtgruppe?
1 ja
2 nein

Störung des öffentlichen Friedens durch Androhung von Straftaten, § 126 StGB

v101 Androhung von Straftaten
1 ja
2 nein

v102 Wenn mittels Endeinrichtung begangen, welche Art von Endeinrichtung?
1 Telefon
2 Handy
3 Fax
4 Computer
0 Sonstige: ....

v103 Kurze Sachverhaltsschilderung: ....

v104 Androhung von Straftaten: Gesamtgruppe?
1 ja
2 nein

Beleidigung

v105 Welche Art:
1 Beleidigung (§ 185 StGB)
2 Üble Nachrede (§ 186 StGB)
3 Verleumdung (§ 187 StGB)
4 Üble Nachrede und Verleumdung gg. Personen des politischen Lebens (§ 188 StGB)
5 Verunglimpfung des Andenkens Verstorbener (§ 189 StGB)

v106 Besondere Art der Beleidigung
1 sexueller Hintergrund
2 rassistischer Hintergrund
0 Sonstiges: ....

v107 Wenn mittels Endeinrichtung begangen, welche Art von Endeinrichtung:
1 Telefon

2 Handy
3 Fax
4 Computer
0 Sonstige:............................

v108 Beleidigung: Gesamtgruppe?
1 ja
2 nein

Verbreiten von Propagandamitteln verfassungswidriger Organisationen, § 86 StGB
v109 Wenn Verbreitung i.S.v. § 86 StGB, welche Art: ....

v110 Verbreitung Propagandamittel: Gesamtgruppe?
1 ja
2 nein

Spezielle Computerkriminalität
v111 Welche Art:
1 Datenveränderung (§ 303a StGB)
2 Computersabotage (§ 303b StGB)
3 Ausspähen von Daten (§ 202a StGB)
4 Softwarepiraterie und sonstige Urheberrechtsverletzungen
0 Sonstiges: ....

v112 Umfang: ....

v113 Spezielle Computerkriminalität: Gesamtgruppe?
1 ja
2 nein

Missbrauch von Notrufen
v114 Missbrauch von Notrufen
1 ja
2 nein

v115 Umfang (*Anzahl der Anrufe*): ....

v116 Missbrauch von Notrufen: Gesamtgruppe?
1 ja
2 nein

Allgemein zu Tatausführungen
v117 Gruppenbegehung
1 ja
2 nein

v118 Anzahl der Beteiligten: ....

v119 Schusswaffen
1 ja
2 nein
3 benutzt (*gedroht*)
4 benutzt (*geschossen*)
5 Scheinwaffe *(mitgeführt)*
6 Scheinwaffe *(gedroht)*

OK-Elemente
v120 Hinweise auf OK-Elemente (*Mehrfachnennungen möglich*)
1 Gewinn- und Machtstreben
2 planmäßige Begehung von Straftaten
3 Erheblichkeit der Straftaten (einzeln oder in der Gesamtheit)

4 mehr als 2 Beteiligte
5 längere/unbestimmte Dauer des Zusammenwirkens
6 arbeitsteiliges Handeln
7 gewerbliche/geschäftsähnliche Strukturen
8 Anwendung von Gewalt/anderen Einschüchterungsmitteln
9 Einflussnahme von Politik, Medien, Justiz oder Wirtschaft (z.B. Korruption)
0 Sonstiges: ....

v121 Hierarchischer Aufbau der Gruppe?
1 ja
2 nein

v122 Deliktischer Schwerpunkt: ....

v123 Räumliche Dimensionen
1 Regional
2 National/mehrere Bundesländer
3 International/grenzüberschreitend

v124 Hinweise auf erzielte Gewinne
1 ja
2 nein

v125 Größenordnung der (*geschätzten*) Gewinne (*in EUR*): ....

Kosten/Dauer/Vernichtung

v126 Konnten in dem Verfahren Verbindungsdaten abgefragt werden:
1 ja
2 nein

v127 Hinweise auf **Vernichtung**
1 ja, alle nicht mehr erforderlichen Unterlagen vernichtet
2 Teilweise vernichtet: ....
3 Keine Vernichtung
4 Keine Hinweise

v128 Vernichtung in Akten vermerkt?
1 ja
2 nein

v129 Datum der Vernichtung: ....

v130 Durch wen erfolgte die Vernichtung?
1 Polizei
2 StA
0 sonstige

v131 Bei Vernichtung durch Polizei: Erfolgte die Vernichtung unter Aufsicht der StA?
1 ja
2 nein

v132 Erfolgte eine Niederschrift über die Vernichtung (§ 100b VI 2 StPO)?
1 ja
2 nein

v133 Gesamtkosten der Auskunftserteilung (*EUR*): ....

v134 Welche Netzanbieter wurden in diesem Verfahren zur Auskunft verpflichtet: (*MN*)
1 Arcor
2 E-Plus
3 o2

4 T-Com
5 T-Mobile
6 Vodafone
0 Sonstige: ....

v135 Netzanbieterkosten (*EUR*): ....

v136 An wen ging die Rechnung der Netzanbieter: ....

v137 In welchem Umfang wurden Netzanbietern Kosten ersetzt: ....

v138 Von wem wurden den Netzanbietern die Kosten ersetzt: ....

v139 sonstige Kosten für Auskunftserteilung (*Grund und Betrag*): ....

v140 Erfolg der Auskunftserteilung
1 ja, in Akte als erfolgreich eingestuft
2 nein, in Akte ausdrücklich als nicht erfolgreich eingestuft
3 ja, nach Einschätzung des Bearbeiters
4 bedingt, nach Einschätzung des Bearbeiters
5 nein, nach Einschätzung des Bearbeiters

Internationale Rechtshilfe

v141 Rechtshilfeersuchen
1 ja
2 nein

v142 Rechtshilfe liegt vor (*durchgeführt*)
1 ja
2 nein

v143 Länder: ....

v144 Rechtshilfeinhalt (*Stichworte*): ....

v145 TK-Daten-bezogene Rechtshilfe?
1 ja
2 nein

v146 Wenn TK-Daten-bezogen
1 Auskunftserteilung im Ausland
2 Auskunftserteilung im Inland

v147 Wesentliches Ergebnis der Rechtshilfe (*in Stichworten*): ....

Sonstige Bemerkungen der Bearbeiterin /des Bearbeiters

v148 Hinweise mit TK-Daten-Bezug (*Autor, Inhalt in Stichworten*):
....
....
....

v149 Sonstige Bemerkungen (*Kurzzusammenfassung und sonstiges*)
....
....
....

Beschluss

v001 Fall_Nr.(*Bearbeiternr.2stellig; Anzahl bearbeiteter Akten 3stellig; z.B. 05025)*: ....

s01 Beschluss_Nr: ....

s01a AZ: ....

s02 Katalogdelikt i.S.v. § 100a StPO (*Mehrfachnennungen möglich*)
1 Friedensverrat, Hochverrat, Landesverrat etc. (§ 100a Satz 1 Nr.1a StPO)
2 Landesverteidigung (§ 100a Satz 1 Nr. 1b StPO)
3 Öffentliche Ordnung (§ 100a Satz 1 Nr. 1c StPO)
4 Fahnenflucht, Anstiftung zum Ungehorsam (§ 100a Satz 1 Nr. 1d StPO)
5 NATO-Truppen (§ 100a Satz 1 Nr. 1e StPO)
6 Geld- oder Wertpapierfälschung (§ 100a Satz 1 Nr.2 StPO)
7 Schw. sex. Missbrauch v. Kindern u. mit Todesfolge (§ 100a Satz 1 Nr. 2 StPO)
8 Verbreitung pornografischer Schriften (§ 100a Satz 1 Nr. 2 StPO)
9 Mord, Totschlag, Völkermord (§ 100a Satz 1 Nr.2 StPO)
10 Straftaten gegen die persönliche Freiheit (§ 100a Satz 1 Nr.2 StPO)
11 Bandendiebstahl, schwerer Bandendiebstahl (§ 100a Satz 1 Nr.2 StPO)
12 Raub, räuberische Erpressung (§ 100a Satz 1 Nr.2 StPO)
13 Erpressung (§ 100a Satz 1 Nr.2 StPO)
14 Gewerbsmäßige Hehlerei, Bandenhehlerei etc. (§ 100a Satz 1 Nr.2 StPO)
15 Geldwäsche, etc. (§ 100a Satz 1 Nr.2 StPO)
16 gemeingefährliche Straftaten (§ 100a Satz 1 Nr.2 StPO)
17 WaffG, Außenwirtschaftsgesetz, KrKG (§ 100a Satz 1 Nr.3 StPO)
18 BtMG (§ 100a Satz 1 Nr.4 StPO)
19 AuslG/AufenthG, AsylVfG (§ 100a Satz 1 Nr.5 StPO)

s03 Andere Straftaten von erheblicher Bedeutung/mittels Endeinrichtung begangene Straftaten
1 Straftaten gegen die sexuelle Selbstbestimmung (§§ 176, 177, 178, 182 StGB)
2 Straftaten gegen die persönliche Freiheit (§§ 232, 233, 234, 235, 236, 239, 240, 241)
3 Diebstahl/Raub (§§ 242, 243, 244 I Nr. 1, 3, 252 StGB)
4 Hehlerei (§ 259 StGB)
5 Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte (nicht § 261 Abs. 1, 2 o. 4 StGB)
6 Gemeingefährliche Straftaten (§§ 315 - nicht Abs.3, 315b - nicht Abs.3, 315c StGB)
7 Verstöße gegen WaffG, die nicht in § 100a Satz 1 Nr. 3 StPO aufgeführt sind
8 Verstöße gegen AußenwirtG, die nicht in § 100a Satz 1 Nr. 3 StPO aufgeführt sind
9 Verstöße gegen BtMG, die nicht in § 100a Satz 1 Nr. 4 StPO aufgeführt sind
10 Verstöße gegen Ausländerrecht, die nicht in § 100a Satz 1 Nr. 5 StPO aufgeführt sind
11 Betrug (§§ 263, 263a StGB)
12 Körperverletzungsdelikte (§§ 223, 224, 226, 227 StGB)
13 Störung des öffentlichen Friedens durch Androhung von Straftaten, § 126 StGB
14 Beleidigung (§§ 185, 186, 187, 188, 189 StGB)
15 Verbreiten von Propagandamitteln verfassungswidriger Organisationen, § 86 StGB
16 Spezielle Computerkriminalität (§§ 303a, 303b, 202a StGB)
17 Missbrauch von Notrufen
0 Sonstiges: ....

s04 Falls mittels Endeinrichtung begangen: mittels welcher
1 Telefon
2 Handy
3 Fax
4 Computer
0 Sonstiges: ....

s05 Ermittlungsstand vor erster Auskunftsanordnung: ....

s06 Datum Anregung: ....

s07 Von wem geht die Initiative zur Antragstellung aus?
1 Polizei
2 Staatsanwaltschaft
3 Richter

s08 Datum Antrag/ Eilmaßnahme: ....

s09 Bezeichnung der Rechtsgrundlage im Antrag:
1 §§ 100g, 100h StPO
2 § 89 TKG (a.F.)/ § 113 TKG (n.F.)
3 §§ 100g, 100h StPO/TKG
4 Sonstiges: ………………….

s10 Wurde §§100gh-Beschluß ursprünglich als erforderlich angesehen?
1 ja
2 nein

s11 Wenn nein, Gründe für §§ 100gh-Beschluss (z.B. Verlangen der Netzbetreiber):
....

s12 Was wurde ursprünglich für ausreichend angesehen? (z.B. § 113 TKG) ....

s13 In welcher staatsanwaltschaftlichen Abteilung wird die Maßnahme beantragt?
1 Organisierte Kriminalität
2 BtM
3 Wirtschaftsdelikte
4 Allgemeines Dezernat/Abteilung
5 Sexualstraftaten
6 Abteilung „Verbreitung kinderpornographischer Schriften“
0 Sonstige: ....

s14 Hinweise auf informelle Besprechungen vor Antragstellung:
1 ja
2 nein

s15 Wenn ja, welchen Inhalt hatten diese: ....

s16 Datum Beschluss (bei Eilanordnung: Datum Bestätigungsbeschluss): ....

s17 Anzahl der Anschlüsse: ....

s18 Ziel der Auskunftsanordnung:
1 Allgemeine Feststellung von Beweismaterial/ Sachverhaltserforschung
2 Spezielle Zielsetzung (für alle Anschlüsse gleich)
3 Spezielle Zielsetzung (anschlussspezifisch)

s19 Polizei-Begründung (*in Stichworten)* ....

s20 Ergebnis der Einschaltung der StA wegen TK-Daten
1 Maßnahme wird beim Richter beantragt
2 Maßnahme wird im Eilverfahren angeordnet
3 Maßnahme wurde nicht angeregt/beantragt, aber vom Richter beschlossen
0 Sonstiges: ....

s21 Begründung des Antrags auf Auskunftserteilung/der Eilanordnung durch StA
1 Formelhaft
2 Vordruck/ Formblatt
3 Verweis auf Polizei-Begründung
4 Begründung mit der Gesetzesformel
5 Substantiell begründet (*z.B. Auseinandersetzung mit anderen Ermittlungsmaßnahmen*
6 Verweis auf Erstbegründung

7 telefonischer Antrag, daher Begründung unbekannt
8 StA schickt Beschluss-Entwurf für Richter mit
0 Sonstiges: ....

s22 StA-Begründung *(in Stichworten)*: ....

s23 Anzahl Zeilen der Antragsgründe: ....

s24 Begründung der richterlichen Entscheidung
1 Formelhaft
2 Vordruck/Formblatt
3 Verweis auf Polizei-Begründung
4 Verweis auf StA-Begründung
5 Begründung mit Gesetzesformel
6 Substantiell begründet *(z.B. Auseinandersetzung mit anderen Erm.möglichkeiten*)
7 Verweis auf Erstbegründung
8 Wie Antrag ausgefertigt
9 Richter unterschreibt lediglich den mitgeschickten Beschluss(entwurf) der StA
0 Sonstiges: ....

s25 Richter-Begründung *(in Stichworten*): ....

s26 Anzahl Zeilen der Beschlussbegründung ....

s27 Bei Eilanordnung: Wann erfolgte richterliche Bestätigung?
1 sofort
2 1 Tag
3 2 Tage
4 3 Tage
5 später: ....
6 Eilanordnung wurde gar nicht bestätigt, aber trotzdem durchgeführt

s28 Wurde Verlängerung beantragt und bewilligt?
1 ja, beantragt und bewilligt
2 ja, beantragt und nicht bewilligt
3 nein, nicht beantragt

s29 Wenn bewilligt: Beschluss_Az (Verlängerung)? ....

s29a Datum des Verlängerungs-Beschlusses: ....

s30 Welche Verlängerungsdauer wurde beantragt? ....

s31 Welche Verlängerungsdauer wurde angeordnet? (*Monate*) ....

s32 Im Falle einer oder mehrfacher Verlängerung: Entscheidet derselbe Richter?
1 ja
2 nein

s33 Wann entscheidet der Richter über die Verlängerung?
1 sofort
2 1 Tag
3 2 Tage
4 3 Tage
0 Sonstiges: ....

s34 Begründung für Verlängerung/Nichtverlängerung?
1 ja
2 nein

s35 Begründung der Verlängerung/Nichtverlängerung?

1 Formelhaft
2 Vordruck/ Formblatt
3 Verweis auf Polizei-Begründung
4 Begründung mit der Gesetzesformel
5 Substantiell begründet (*z.B. Auseinandersetzung mit anderen Ermittlungsmaßnahmen*)
6 Verweis auf Erstbegründung
0 Sonstiges: ....

s36 Begründung der (Nicht-)Verlängerung (Stichworte):..

s37 Welche Art von Auskunftserteilung: (*MN möglich*)
1 gerichtet auf vorhandene Verbindungsdaten
2 gerichtet auf zukünftige Verbindungsdaten
3 Zielwahlsuche
4 Funkzellenabfrage
0 Sonstiges: ....

s38 Durch wen erfolgt die Anforderung der Daten bei den Netzbetreibern?
1 Polizei
2 Staatsanwaltschaft
3 Richter

s39 Welche Netzanbieter wurden durch diesen Beschluss zur Auskunft verpflichtet: (*MN möglich*)
1 Arcor
2 E-Plus
3 o2
4 T-Com
5 T-Mobile
6 Vodafone
0 Sonstige: ....

s39a Haben die Netzbetreiber den Beschluss ohne Gründe erhalten?
1 ja
2 nein

s40 Welche Netzbetreiber weigerten sich Auskunft zu erteilen?
1 Arcor
2 E-Plus
3 o2
4 T-Com
5 T-Mobile
6 Vodafone
0 Sonstige: ....

s41 Grund für die Weigerung: ....

s42 Wurden Ordnungs- oder Zwangsmittel gegen die Netzbetreiber verhängt?
1 ja
2 nein
3 teilweise: ....

s43 Kam es zu zeitlichen Verzögerungen?
1 ja
2 nein
3 teilweise: ....

s44 Wenn ja, aus welchem Grund: ....

s45 Haben Netzbetreiber Rechtsmittel gegen Anordnung eingelegt? (*Welcher Netzbetreiber, Art des Rechtsmittels, Datum, Ergebnis*): ....
....

s46 Bei welchen Netzanbietern sind Verbindungsdaten entstanden?
1 Arcor
2 E-Plus
3 o2
4 T-Com
5 T-Mobile
6 Vodafone
0 Sonstige: ....

s46a Befindet sich eine Auflistung der Verbindungsdaten in der Akte?
1 ja
2 nein

s47 Gesamtkosten der Auskunftserteilung für diesen Beschluss (EUR): ....

s48 Kosten der Netzanbieter (EUR):
1 Arcor : ....
2 E-Plus : ....
3 o2 : ....
4 T-Com : ....
5 T-Mobile : ....
6 Vodafone: ....
0 Sonstige: ....

s49 An wen ging die Rechnung der Netzanbieter: ....

s49a Datum der Rechnung des Netzanbieters:
1 Arcor : ....
2 E-Plus : ....
3 o2 : ....
4 T-Com : ....
5 T-Mobile : ....
6 Vodafone: ....
0 Sonstige: ....

s50 In welchem Umfang wurden Netzanbietern Kosten ersetzt: ....

....

s51 Von wem wurden den Netzanbietern die Kosten ersetzt: ....

s51a Datum der Zahlungsveranlassung (z.B. durch die StA): ....
1 Arcor : ....
2 E-Plus : ....
3 o2 : ....
4 T-Com : ....
5 T-Mobile : ....
6 Vodafone: ....
0 Sonstige: ....

s51b Datum der Kassenanweisung/Anweisung der Überweisung der Kosten:
1 Arcor : ....
2 E-Plus : ....
3 o2 : ....
4 T-Com : ....
5 T-Mobile : ....
6 Vodafone: ....
0 Sonstige: ....

s52 sonstige Kosten (*Grund und Betrag*): ....

s53 Hinweise auf gesonderte **Benachrichtigung der Betroffenen**

1 Keine besonderen Hinweise
2 Benachrichtigung ist erfolgt
3 Keine Benachrichtigung
4 Zurückstellung der Benachrichtigung (*z.B.101 StPO*)
5 Sonstige Kenntniserlangung durch Strafverfolgungsbehörde
(*z.B. Vorhalt; Akteneinsicht*) ....

s54 Wenn keine Benachrichtigung: Wurde Grund angegeben?
1 ja: ....
2 nein

s55 Datum Benachrichtigung: ....

s56 Wie viele Personen waren von der Auskunftserteilung betroffen: ....

s57 Wie viele Personen davon waren Beschuldigte: ....

s58 Wie viele Betroffene wurden benachrichtigt: ....

s59 Wer wurde benachrichtigt:
1 Beschuldigte (Beschuldigten_Nr.): ....
2 Anschlussinhaber (Anschluß_Nr.): ....
3 Dritter: ....
0 Sonstiges: ....

s60 Wurden vor Anregung/Anordnung der Auskunftserteilung andere Ermittlungsmaßnahmen anstelle der Auskunftserteilung in Betracht gezogen?
1 ja
2 nein

s61 Welche sind dies und warum wurden sie nicht angeordnet: ....

s62 Wurden durch diesen Beschluss Verbindungsdaten, die <u>von</u> dem Anschluss eines Zeugnisverweigerungsberechtigten ausgehen, abgefragt? (*Art des ZVR*)
1 Verlobte (§ 52 I Nr. 1 StGB)
2 Ehegatte (/Exehegatte)/Lebenspartner (§ 52 I Nr. 2 u. 2a StGB)
3 Verwandte (§ 52 I Nr. 3StGB)
4 Geistliche (§ 53 I Satz 1 Nr. 1 StGB)
5 Verteidiger (§ 53 I Satz 1 Nr. 2 StGB)
6 Rechtsanwälte, Patentanwälte, Notare (§ 53 I Satz 1 Nr. 3 StGB)
7 Wirtschaftsprüfer, Steuerberater (§ 53 I Satz 1 Nr. 3 StGB)
8 Ärzte (§ 53 I Satz 1 Nr. 3 StGB)
9 Psychotherapeuten (§ 53 I Satz 1 Nr. 3 StGB)
10 Apotheker, Hebammen (§ 53 I Satz 1 Nr. 3 StGB)
11 Berater nach SchwangerschaftskonflG und für BtM (§ 53 I Satz 1 Nr. 3a und 3b StGB)
12 Mitglieder des Bundestages und der Landtage (§ 53 I Satz 1 Nr. 4 StGB)
13 Journalisten (§ 53 I Satz 1 Nr. 5 StGB)
14 Berufshelfer (§ 53a StGB)

s63 Schilderung des Zeugnisverweigerungsrechts/Sachverhalts in Stichworten:................................
....

s64 War das Zeugnisverweigerungsrecht vor der Anordnung ersichtlich?
1 ja
2 nein

s65 Wurden durch diesen Beschluss Verbindungsdaten <u>zu</u> dem Anschluss eines Zeugnisverweigerungsberechtigten abgefragt? (*Art des ZVR*)
1 Verlobte (§ 52 I Nr. 1 StGB)
2 Ehegatte (/Exehegatte)/Lebenspartner (§ 52 I Nr. 2 u. 2a StGB)
3 Verwandte (§ 52 I Nr. 3StGB)
4 Geistliche (§ 53 I Satz 1 Nr. 1 StGB)

5 Verteidiger (§ 53 I Satz 1 Nr. 2 StGB)
6 Rechtsanwälte, Patentanwälte, Notare (§ 53 I Satz 1 Nr. 3 StGB)
7 Wirtschaftsprüfer, Steuerberater (§ 53 I Satz 1 Nr. 3 StGB)
8 Ärzte (§ 53 I Satz 1 Nr. 3 StGB)
9 Psychotherapeuten (§ 53 I Satz 1 Nr. 3 StGB)
10 Apotheker, Hebammen (§ 53 I Satz 1 Nr. 3 StGB)
11 Berater nach SchwangerschaftskonflG und für BtM (§ 53 I Satz 1 Nr. 3a und 3b StGB)
12 Mitglieder des Bundestages und der Landtage (§ 53 I Satz 1 Nr. 4 StGB)
13 Journalisten (§ 53 I Satz 1 Nr. 5 StGB)
14 Berufshelfer (§ 53a StGB)

s66 Schilderung des Zeugnisverweigerungsrechts/Sachverhalts in Stichworten:................................
....

s67 War das Zeugnisverweigerungsrecht vor der Anordnung ersichtlich?
1 ja
2 nein

s68 Bestand ein Verwertungsverbot?
1 ja
2 nein

s69 Wenn ja: Wurden die Daten trotzdem verwertet?
1 ja
2 nein

s70 Schilderung des Sachverhalts bzgl. des Verwertungsverbots:...
....

s71 Anmerkungen (*zum Beschluss*):...

s72 Gegen welchen Beschuldigten richtet sich der Beschluss? (*MN*) ....

Anschluss

v001 Fall_Nr.: *(Bearbeiternr.2stellig; Anzahl bearbeiteter Akten 3stellig; z.B. 05025)*:.......................

s01 Beschluss_Nr: ....

a01 Anschluss_Nr: ....

a02 Art des Anschlusses/der Nutzung
1 Festnetz/privat
2 Festnetz/Betrieb
3 Mobiltelefon
4 Öffentlicher Anschluss
5 Scall
6 Fax
7 E-Mail
8 SMS
9 Mailbox
10 P2P-Dienste
11 VoIP-Dienste
12 andere WWW-Dienste
0 Sonstige: ....

a03 Wie viele Anschlussinhaber sind betroffen: ....

a04 Verbindungsdatenabfrage zu: (*MN möglich*)
1 Rufnummer

2 IP-Adresse
3 IMEI-Nummer
0 Sonstiges: ....

a05 Handelt es sich um einen ISDN-Anschluss
1 ja
2 nein

a06 Anzahl der überprüften Rufnummern (*bei ISDN*): ....

a07 Anzahl der überprüften IP-Adressen: ....

a08 Anzahl der überprüften IMEI-Nr.: ....

a09 Falls IP-Adressen überprüft wurden, welche Art:
1 statische IP-Adressen
2 dynamische IP-Adressen

a10 Welche Art von Auskunftserteilung: (*MN möglich*)
1 gerichtet auf vorhandene Verbindungsdaten
2 gerichtet auf zukünftige Verbindungsdaten
3 Zielwahlsuche
4 Funkzellenabfrage
0 Sonstiges: ....

a11 Wurde anhand der vorhandenen IP-Adresse die Rufnummer abgefragt?
1 ja
2 nein

a12 Wurde anhand der vorhandenen Rufnummer die IP-Adresse abgefragt?
1 ja
2 nein

a13 Was wurde genau abgefragt?
1 Berechtigungskennungen
2 Kartennummern
3 Standortkennung
4 Rufnummer des angerufenen Anschlusses
5 Rufnummer des anrufenden Anschlusses
6 Kennung (z.B. IP-Adresse) des angerufenen Anschlusses
7 Kennung (z.B. IP-Adresse) des anrufenden Anschlusses
8 Beginn und Ende von Verbindungen
9 der vom Nutzer in Anspruch genommene Telekommunikationsdienst
10 Endpunkte festgeschalteter Verbindungen, ihr Beginn/Ende nach Datum und Uhrzeit
11 alle og. Daten
12 allgemein Verbindungsdaten
0 Sonstiges: ....

a14 Dauer laut Antrag (*in Stunden/Tagen/Monaten*): ....

a15 Ziel der Auskunftserteilung (Antrag)
1 Identifizierung des Beschuldigten
2 Feststellung von (weiteren) Anschlüssen des Beschuldigten
3 Bestimmung des Standorts des Beschuldigten zur Tatzeit
4 Ermittlung des aktuellen Aufenthaltsortes
5 Bestimmung der Tatzeit
6 Feststellung von Kommunikationspartnern des Beschuldigten
7 Feststellung weiterer Tatbeteiligter
8 Ermittlung der Anschlüsse weiterer Tatverdächtiger
9 Bewegungsbild
11 Feststellung Rufnummer/IP-Adresse für Folge-Auskunftserteilung
12 Sicherung von Beweisen

	13	Feststellung, ob TKÜ erfolgversprechend ist
	14	Feststellung, ob eine andere Ermittlungsmaßnahme als TÜ in Betracht kommt
	0	Sonstige
a16	Ergebnis des Antrags	
	1	Richter erlässt Maßnahme wie beantragt
	2	Richter ordnet Maßnahme mit Änderungen an
	3	Richter ordnet Maßnahme mit Ergänzungen an
	4	Richter lehnt Maßnahme ab
	5	Richter bestätigt Eilmaßnahme
	6	Richter bestätigt Eilmaßnahme nicht
	7	Beschluss fehlt
	8	Maßnahme war nicht beantragt, nur Beschluss
a17	Inhalt der Änderungen	
	1	Dauer
	2	Umfang
a18	Inhalt der Ergänzungen	
	1	Dauer
	2	Umfang
a19	Welche Änderungen/Ergänzungen:	
a20	Auskunftserteilung abgelehnt:	
	1	ja
	2	nein
a21	Wenn ja, aus welchem Grund:	
	1	Kein ausreichender Tatverdacht
	2	Keine Straftat von *erheblicher* Bedeutung
	3	Milderes Mittel anwendbar
	4	Maßnahme verspricht keinen Erfolg
	0	Sonstiges: ....
a22	Datum der Ablehnung:	
a23	Auskunftserteilung ausgeführt	
	1	ja
	2	nein
a24	Ausführungsbeginn (*Datum*):..	
a25	Ausführungsende oder –abbruch (*Datum*):	
a25a	Datum der Auskunft (Datum des Schreibens der Anbieter):	
	1	Arcor : ....
	2	E-Plus : ....
	3	o2 : ....
	4	T-Com : ....
	5	T-Mobile : ....
	6	Vodafone: ....
	0	Sonstige: ....
a26	Auskunftserteilung abgebrochen	
	1	ja
	2	nein
a27	Grund des Abbruchs	
	1	Betroffener stellt sich auf Verbindungsdatenüberwachung ein
	2	Andere Maßnahmen führen zum Anordnungsziel
	3	Tatverdacht wegen Anlassdelikt erledigt sich

4 Ergebnis wird nicht mehr erwartet
5 Auskunftserteilung hat angestrebtes Ergebnis bereits erbracht
6 Anschluss wird abgeschaltet
7 SV-Aufklärung mit den zur Verfügung stehenden Mittel nicht möglich
8 keine Gesprächsaktivität (bei Handy: möglicherweise Kartenwechsel)
9 Unterbrechung für einige Tage
0 Sonstiges: ....

a28 Konnten für den Anschluss Verbindungsdaten abgefragt werden:
1 ja: (*Art*) ....
2 nein

a29 Umfang der Verbindungsdaten (Seiten): ....

a30 Bei welchem Anbieter (*Mehrfachnennungen möglich*):
1 Arcor
2 E-Plus
3 o2
4 T-Com
5 T-Mobile
6 Vodafone
0 Sonstige: ....

a31 Hinweise auf technische Probleme
1 ja
2 nein

a32 Wenn ja, welcher Art: ....

a33 Wurden auch die Personendaten hinter einer IP-Adresse/Rufnummer abgefragt?
1 ja
2 nein

a34 Wenn ja, aufgrund welcher Rechtsgrundlage: ....

a35 Wenn Personendaten hinter einer IP-Adresse abgefragt wurden, welche Art von IP-Adresse:
1 statische IP-Adresse
2 dynamische IP-Adresse

a36 Wie lange wurden die Daten für diesen Anschluss bei welchen Telekommunikationsanbietern nach der Rechnungslegung gespeichert?
1 Arcor : ....
2 E-Plus : ....
3 o2 : ....
4 T-Com : ....
5 T-Mobile : ....
6 Vodafone: ....
0 Sonstige: ....

a37 Erfolgte eine Aufforderung zur längeren Datenspeicherung durch die Polizei/StA?
1 ja (*bei welchem Anbieter*): ....
2 nein

a38 Sind folgende Probleme aufgetreten bzw. liegen Hinweise dafür vor
1 Daten wurden gar nicht gespeichert: ....
2 Daten wurden teilanonymisiert gespeichert: ....
3 Daten wurden zu kurz gespeichert: ....
4 Daten wurden durch Anonymisierungsdienste/Kryptographie verschlüsselt: ....
0 Sonstiges: ....

a39 TK-Daten-Erfolg

6 ja, in Akte als erfolgreich eingestuft
7 nein, in Akte ausdrücklich als nicht erfolgreich eingestuft
8 ja, nach Einschätzung des Bearbeiters
9 bedingt, nach Einschätzung des Bearbeiters
10 nein, nach Einschätzung des Bearbeiters

a40 Formulierung des Erfolges (*Stichworte*): ....
....

Inhaber

v001 Fall_Nr. *(Bearbeiternr.2stellig; Anzahl bearbeiteter Akten 3stellig; z.B. 05025)*: ....

s01 Beschluss_Nr.: ....

a01 Anschluss_Nr.: ....

b01 Beschuldigten_Nr.: ....

ab01 Anschlussinhaber:
1 Beschuldigter
2 Scheindritter: Beschuldigter unter fremdem Namen
3 Dritter
4 Dritter und Beschuldigter
5 Anschlussinhaber nicht festgestellt

ab02 Nutzung
1 durch den Beschuldigten
2 auch durch den Dritten
3 nur durch den Dritten

ab03 Verhältnis Anschlussinhaber - Beschuldigter
1 Familie
2 Verwandtschaft
3 Freunde/Bekannte
4 Beruf-Arbeitgeber
5 Beruf-Arbeitskollegen
6 Szenebekanntschaft (Drogen)
7 ethnische Beziehung (*gleiche Ethnie*)
8 keine Beziehung
9 Kontaktperson
10 Nachrichtenmittler
0 Sonstiges: ....

ab04 Verhältnis Anschlussinhaber/ weiterer Inhaber
1. Ehepaar
2. WG
3. Kollegen
4. Sonstiges: ....

ab05 Zeugnisverweigerungsrecht des Anschlussinhabers (im Verhältnis zum Beschuldigten)
1 ja
2 nein

ab06 Wenn ja, welches:
1 Verlobte (§ 52 I Nr. 1 StGB)
2 Ehegatte (/Exehegatte)/Lebenspartner (§ 52 I Nr. 2 u. 2a StGB)
3 Verwandte (§ 52 I Nr. 3StGB)
4 Geistliche (§ 53 I Satz 1 Nr. 1 StGB)
5 Verteidiger (§ 53 I Satz 1 Nr. 2 StGB)
6 Rechtsanwälte, Patentanwälte, Notare (§ 53 I Satz 1 Nr. 3 StGB)

7 Wirtschaftsprüfer, Steuerberater (§ 53 I Satz 1 Nr. 3 StGB)
8 Ärzte (§ 53 I Satz 1 Nr. 3 StGB)
9 Psychotherapeuten (§ 53 I Satz 1 Nr. 3 StGB)
10 Apotheker, Hebammen (§ 53 I Satz 1 Nr. 3 StGB)
11 Berater nach SchwangerschaftskonflG und für BtM (§ 53 I Satz 1 Nr. 3a und 3b StGB)
12 Mitglieder des Bundestages und der Landtage (§ 53 I Satz 1 Nr. 4 StGB)
13 Journalisten (§ 53 I Satz 1 Nr. 5 StGB)
14 Berufshelfer (§ 53a StGB)

ab07 Schilderung des Zeugnisverweigerungsrechts/Sachverhalts in Stichworten:................................
....

ab08 War das Zeugnisverweigerungsrecht vor der Anordnung ersichtlich?
1 ja
2 nein

ab09 Bestand ein Verwertungsverbot?
1 ja
2 nein

ab10 Wenn ja: Wurden die Daten trotzdem verwertet?
1 ja
2 nein

ab11 Um welche Art der Verbindung handelt es sich?
1 Verbindungen von dem Anschluss des Anschlussinhabers
2 Verbindungen zu dem Anschluss des Anschlussinhabers

ab12 War der Anschlussinhaber mit der Abfrage seiner Verbindungsdaten einverstanden?
1 ja
2 nein
3 vermutlich ja

Beschuldigte

v001 Fall_Nr.(*Bearbeiternr.2stellig;Anzahl bearbeiteter Akten 3stellig:z.B. 05025):*...........................

b01 Beschuldigten_Nr: ....

b02 Staatsangehörigkeit: ....

b03 Geburtsjahr des Beschuldigten (*4 Stellen*): ....

b04 Geschlecht
1 männlich
2 weiblich

b05 Familienstand
1 ledig
2 verheiratet
3 geschieden
4 verwitwet

b06 Vorstrafen
1 ja
2 nein

b07 Anzahl Vorstrafen/Delikte: ....

b08 Gesamtdauer der verhängten Vorstrafen (*in Monaten*) ....

b09 Gesamthöhe der verhängten Geldstrafen (*Anzahl der Tagessätze*) ....

b10 Vollzugserfahrung
1 ja
2 nein

b11 ausgeübter Beruf (*wenn nicht feststellbar: erlernter*) ....

b12 Kenntniserlangung des verfahrensauslösenden Sachverhalts durch Polizei (*Datum*): ....

b13 OK-Element: Stellung des TV in der Gruppe
1 Leitung
2 Mittlerer Bereich
3 Ausführend

b14 OK-Element: Entstehung der Täterverbindungen
1 JVA
2 Milieu
3 Drogenszene
4 Ethnie/Nationalität
5 Familie
0 Sonstiges: ....

b15 Katalogdelikt i.S.v. § 100a StPO (*Mehrfachnennungen möglich*) (Ermittlungsdelikte!)
1 Friedensverrat, Hochverrat, Landesverrat etc. (§ 100a Satz 1 Nr.1a StPO)
2 Landesverteidigung (§ 100a Satz 1 Nr. 1b StPO)
3 Öffentliche Ordnung (§ 100a Satz 1 Nr. 1c StPO)
4 Fahnenflucht, Anstiftung zum Ungehorsam (§ 100a Satz 1 Nr. 1d StPO)
5 NATO-Truppen (§ 100a Satz 1 Nr. 1e StPO)
6 Geld- oder Wertpapierfälschung (§ 100a Satz 1 Nr.2 StPO)
7 Schw. sex. Missbrauch v. Kindern u. mit Todesfolge (§ 100a Satz 1 Nr. 2 StPO)
8 Verbreitung pornografischer Schriften (§ 100a Satz 1 Nr. 2 StPO)
9 Mord, Totschlag, Völkermord (§ 100a Satz 1 Nr.2 StPO)
10 Straftaten gegen die persönliche Freiheit (§ 100a Satz 1 Nr.2 StPO)
11 Bandendiebstahl, schwerer Bandendiebstahl (§ 100a Satz 1 Nr.2 StPO)
12 Raub, räuberische Erpressung (§ 100a Satz 1 Nr.2 StPO)
13 Erpressung (§ 100a Satz 1 Nr.2 StPO)
14 Gewerbsmäßige Hehlerei, Bandenhehlerei etc. (§ 100a Satz 1 Nr.2 StPO)
15 Geldwäsche, etc. (§ 100a Satz 1 Nr.2 StPO)
16 gemeingefährliche Straftaten (§ 100a Satz 1 Nr.2 StPO)
17 WaffG, Außenwirtschaftsgesetz, KrKG (§ 100a Satz 1 Nr.3 StPO)
18 BtMG (§ 100a Satz 1 Nr.4 StPO)
19 AuslG/AufenthG, AsylVfG (§ 100a Satz 1 Nr.5 StPO)

b16 Andere Straftaten von erheblicher Bedeutung/mittels Endeinrichtung begangene Straftaten
1 Straftaten gegen die sexuelle Selbstbestimmung (§§ 176, 177, 178, 182 StGB)
2 Straftaten gegen die persönliche Freiheit (§§ 232, 233, 234, 235, 236, 239, 240, 241)
3 Diebstahl/Raub (§§ 242, 243, 244 I Nr. 1, 3, 252 StGB)
4 Hehlerei (§ 259 StGB)
5 Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte (nicht § 261 Abs. 1, 2 o. 4 StGB)
6 Gemeingefährliche Straftaten (§§ 315 - nicht Abs.3, 315b - nicht Abs.3, 315c StGB)
7 Verstöße gegen WaffG, die nicht in § 100a Satz 1 Nr. 3 StPO aufgeführt sind
8 Verstöße gegen AußenwirtG, die nicht in § 100a Satz 1 Nr. 3 StPO aufgeführt sind
9 Verstöße gegen BtMG, die nicht in § 100a Satz 1 Nr. 4 StPO aufgeführt sind
10 Verstöße gegen Ausländerrecht, die nicht in § 100a Satz 1 Nr. 5 StPO aufgeführt sind
11 Betrug (§§ 263, 263a StGB)
12 Körperverletzungsdelikte (§§ 223, 224, 226, 227 StGB)
13 Störung des öffentlichen Friedens durch Androhung von Straftaten, § 126 StGB
14 Beleidigung (§§ 185, 186, 187, 188, 189 StGB)
15 Verbreiten von Propagandamitteln verfassungswidriger Organisationen, § 86 StGB
16 Spezielle Computerkriminalität (§§ 303a, 303b, 202a StGB)

17 Missbrauch von Notrufen
0 Sonstiges: ....

b17 Falls mittels Endeinrichtung begangen: mittels welcher
1 Telefon
2 Handy
3 Fax
4 Computer
0 Sonstiges: ....

b18 Untersuchungshaft
1 ja
2 nein

b19 Beginn der Untersuchungshaft *(Datum):* ....

b20 Dauer der Untersuchungshaft (*bis Beginn Hauptverhandlung in Tagen*) ....

b21 Haftverschonung
1 ja
2 nein
3 ja, aber nur vorübergehend

b22 Verteidiger vorhanden?
1 ja , Wahlverteidiger
2 ja , Pflichtverteidiger
3 ja , zuerst Wahlverteidiger, dann Pflichtverteidiger
4 nein

b23 Datum der Einschaltung eines Verteidigers: ....

b24 Datum erste Beschuldigtenvernehmung: ....

b25 Geständnis des Tatverdächtigen
1 ja, in vollem Umfang der Tatvorwürfe
2 ja, teilweise
3 nein
4 ja, aber Widerruf

b26 Zeitpunkt des Geständnisses: ....

b27 Einstellung/Anklage/Strafbefehl
1 Einstellung
2 Teileinstellung
3 Anklage
4 Strafbefehl

b28 In Anklage/Strafbefehl aufgeführte Beweismittel *(in Stichworten)*: ....

b29 Stellenwert der Auskunftserteilung in der Anklage/Strafbefehl? ....

b30 Anklage zum
1 Einzelrichter AG
2 Schöffengericht
3 Große Strafkammer
4 Wirtschaftsstrafkammer
5 OLG-Senat
6 Jugendrichter
7 Jugendschöffengericht
8 Jugendkammer

b31 Beginn der Hauptverhandlung *(Datum):* ....

b32 Ende der Hauptverhandlung *(Datum):* ....

b33 Protokoll in der Akte enthalten
1 ja
2 nein
3 Auszüge

b34 Hinweise auf Absprachen
1 ja
2 nein

b35 Wenn ja
1 Explizit angesprochen
2 Indizien (wie z.B. StA und Verteidigung stellen gleichen Strafantrag): ....
0 Sonstiges: ....

b36 Einlassung des Angeklagten
1 Geständnis
2 Teilgeständnis
3 Bestreiten
4 Schweigen

b37 HV_Nr.: ....

b38 Zeugenvernehmung
1 ja
2 nein

b39 Anzahl der Zeugen ....

b40 Werden die Verbindungsdaten als Beweismittel eingeführt?
1 ja
2 nein

b41 Einführung zum Beweis von: ....

b42 Einführung sonstiger Beweismittel
1 ja: ....
2 nein

b43 Beweisanträge durch die StA
1 ja
2 nein

b44 Beweisanträge TK-Daten-bezogen?
1 ja
2 nein

b45 Wenn TK-Daten-bezogen, Inhalt: ....

b46 Stellenwert der Auskunftserteilung bei den Beweisanträgen im Vergleich zu anderen Beweismitteln: ....

b47 Beweisanträge der Verteidigung
1 ja
2 nein

b48 Beweisanträge der Verteidigung TK-Daten-bezogen?
1 ja
2 nein

b49 Wenn Anträge TK-Daten-bezogen, Inhalt: ....

b50 Urteilsinhalt
1 Freispruch
2 Verurteilung
3 Einstellung (*nach Anklageerhebung*)
4 Teilfreispruch (*Delikt*): ....
5 Teileinstellung (*nach Anklageerhebung*)

b51 Verurteilungsinhalt
1 Geldstrafe
2 Unbedingte Freiheitsstrafe
3 Bewährungsstrafe
4 Erziehungsmaßregeln
5 Zuchtmittel
6 Jugendstrafe
7 Vorbewährung (§ 57 JGG)

b52 Freiheitsstrafe Dauer (*in Monaten, bei lebenslanger Freiheitsstrafe 900*): ....

b53 Geldstrafe Anzahl Tagessätze u. Höhe des Tagessatzes: ....

b54 Bewährung
1 ja
2 nein

b55 Auflagen/Weisungen (*welche Art*)?...

b56 Wenn ja, welcher Umfang (*EUR/Stunden*): ....

b57 Dauer der Bewährungszeit (*in Monaten*) ....

b58 Maßregeln der Besserung und Sicherung (*Mehrfachnennungen möglich*)
1 Unterbringung in einem psychiatrischen Krankenhaus
2 Unterbringung in einer Entziehungsanstalt
3 Unterbringung in der Sicherungsverwahrung
4 Führungsaufsicht
5 Entziehung der Fahrerlaubnis
6 Berufsverbot

b59 Dauer der Maßnahme (*Wochen*): ....

b60 Einziehung (Tatmittel o.ä.)
1 ja
2 nein

b61 Verfall (eines Gewinns o.ä.)
1 ja
2 nein

b62 Höhe der verfallenen Beträge (*in EUR*)? ....

b63 Verfall/Einziehung realisiert?
1 ja
2 teilweise: ....
3 nein
0 Sonstiges (z.B. Verzichtserklärung des Verurteilten): ....

b64 Urteilsbegründung in der Akte vorhanden
1 ja
2 nein
3 Auszüge

b65 Urteilsbegründung

1 abgekürzt
2 Volle Begründung

b66 Anzahl der Seiten der Urteilsbegründung: ....

b67 Davon Seiten Beweiswürdigung: ....

b68 Wird in der Beweiswürdigung die Auskunftserteilung aufgegriffen?
1 ja
2 nein

b69 Mit welcher Beweisrichtung wird die Auskunftserteilung aufgegriffen?
1 Belastend (*voller Nachweis der Täterschaft*)
2 Belastend im Zusammenhang mit anderen Beweismitteln
3 Entlastend
4 Ohne Beweiskraft

b70 Stellenwert der Auskunftserteilung (*Einschätzung*)...

b71 Ausländerbehörde involviert?
1 ja
2 nein

b72 Ausweisung/Abschiebung hat stattgefunden?
1 hat stattgefunden
2 ist angeordnet
3 ist eingeleitet

b73 Anwendung § 456a StPO
1 ja
2 nein

b74 Anmerkungen (*zum Beschuldigten*): ....

Anklage + Urteil-Delikt

v001 Fall_Nr.(*Bearbeiternr.2stellig; Anzahl bearbeiteter Akten 3stellig; z.B.05025)*: ....

b01 Beschuldigten_Nr.: ....

ad01 Delikt (welches Einstellung/Anklage/Strafbefehlsantrag zugrunde liegt): ....

ad02 Anzahl der Fälle: ....

ad03 Einstellung/Anklage/Strafbefehlsantrag
1 Einstellung
2 Teileinstellung
3 Anklage
4 Strafbefehl

ad04 Datum der Einstellung/der Anklage/des Strafbefehlsantrags: ....

ad05 Einstellungsgrundlage
1 § 153 Abs. 1 StPO
2 § 153a Abs. 1 StPO
3 § 153d Abs. 1 StPO
4 § 154 Abs. 1 StPO
5 § 154a Abs. 1 StPO
6 § 154b Abs. 1 bis 3 StPO
7 § 170 II StPO
8 § 45 JGG

9 § 47 JGG
0 Sonstiges: ....

ad06 Begründung der Einstellung (*in Stichworten):* ....

ad07 Identität Anklagedelikt-Anlassdelikt für die Auskunftserteilung
1 ja
2 teilweise: ....
3 nein

ad08 Versuch/Vollendung des Anklagedelikts
1 Vollendung
2 Versuch
3 Verabredung

ad09 Unterlassen (§ 13 StGB)
0 ja
1 nein

ad10 Täterschaft (§ 25 StGB)
1 unmittelbar
2 mittelbar
3 Mittäter

ad11 Beteiligung (§§ 26, 27 StGB)
1 Anstiftung
2 Beihilfe

ad12 Identität Verurteilungsdelikt - Anlassdelikt für die Auskunftserteilung
1 ja
2 teilweise: ....
3 nein

ad13 Identität Anklagedelikt - Verurteilungsdelikt
1 ja
2 geändert
3 weggefallen

ad14 Einstellung nach Anklageerhebung
1 Einstellung
2 Teileinstellung
3 Keine Einstellung

ad15 Einstellungsgrundlage
1 § 153 Abs. 2 StPO
2 § 153a Abs. 2 StPO
3 § 153d Abs. 2 StPO
3 § 154 Abs. 2 StPO
4 § 154a Abs. 2 StPO
5 § 154b Abs. 4 StPO
0 Sonstiges: ....

ad16 Begründung der Einstellung (*in Stichworten):* ....

ad17 Datum der Einstellung: ....

ad18 Verurteilungs(/Strafbefehls-)delikt: ....

ad19 Anzahl der Fälle: ....

ad20 Datum der Verurteilung: ....

ad21 Versuch/Vollendung
1 Vollendung
2 Versuch
3 Verabredung

ad22 Unterlassen (§ 13 StGB)
1 ja
2 nein

ad23 Täterschaft (§ 25 StGB)
1 unmittelbar
2 mittelbar
3 Mittäter

ad24 Beteiligung (§§ 26, 27 StGB)
1 Anstiftung
2 Beihilfe

Rechtsmittel

v001 Fall_Nr.(*Bearbeiternr.2stellig;Anzahl bearbeiteter Akten 3stellig:z.B. 05025):*..........................

b01 Beschuldigten_Nr.: ....

r01 Rechtsmittel_Nr.: ....

r02 Rechtsmittelverfahren
1 nein
2 Rechtsmittelverzicht von beiden Seiten
3 ja, Berufung
4 ja, Revision
5 Berufung zurückgenommen
6 Revision zurückgenommen

r03 Rechtsmittel eingelegt durch
1 Verurteilter
2 Staatsanwalt
3 Beide
4 Nebenkläger

r04 Rücknahme von
1 Verurteilter
2 Staatsanwalt
3 Beide
4 Nebenkläger

r05 Rechtsmittelbegründung in der Akte vorhanden
1 ja
2 nein
3 Auszüge

r06 Rechtsmittelbegründung: Bezug zur Auskunftserteilung?
1 ja
2 nein

r07 Wenn ja, welcher: ....

r08 Ergebnis des Rechtsmittels (*MN möglich*)
1 Bestätigung des erstinstanzlichen Urteils
2 Aufhebung und Zurückverweisung
3 Abänderung in Berufung
4 Verwerfung

0 Sonstiges: ....

r09 Wenn Aufhebung/Abänderung: Zusammenhang mit Auskunftserteilung und wenn ja welcher?
1 ja: ....
2 nein

r10 Wenn Abänderung, welche Verurteilungsdelikte liegen vor?
....

r11 Urteilsinhalt
1 Freispruch
2 Verurteilung
3 Einstellung
4 Teilfreispruch
5 Teileinstellung

r12 Verurteilungsinhalt
1 Geldstrafe
2 Unbedingte Freiheitsstrafe
3 Bewährungsstrafe
4 Erziehungsmaßregeln
5 Zuchtmittel
6 Jugendstrafe
7 Vorbewährung (§ 57 JGG)

r13 Freiheitsstrafe Dauer (*in Monaten, bei lebenslanger Freiheitsstrafe 900*): ....

r14 Geldstrafe Anzahl Tagessätze: ....

r15 Geldstrafe Höhe des Tagessatzes (*in EUR):* ....

r16 Bewährung
1 ja
2 nein

r17 Auflagen/Weisungen (*welche Art*)? ....

r18 Wenn ja, welcher Umfang (*EUR*): ....

r19 Wenn ja, welcher Umfang (*Stunden*): ....

r20 Dauer der Bewährungszeit (*in Monaten*): ....

r21 Maßregeln der Besserung und Sicherung (*Mehrfachnennungen möglich*)
1 Unterbringung in einem psychiatrischen Krankenhaus
2 Unterbringung in einer Entziehungsanstalt
3 Unterbringung in der Sicherungsverwahrung
4 Führungsaufsicht
5 Entziehung der Fahrerlaubnis
6 Berufsverbot

r22 Dauer der Maßnahme (*Wochen*): ....

r23 Einziehung (Tatmittel o.ä.)
1 ja
2 nein

r24 Verfall (eines Gewinns o.ä.)
1 ja
2 nein

r25 Höhe der verfallenen Beträge (*in EUR*)? ....

r26 Verfall/Einziehung realisiert?
1 ja
2 teilweise: ....
3 nein
0 Sonstiges (z.B. Verzichtserklärung des Verurteilten): ....

r27 Urteilsbegründung in der Akte vorhanden
1 ja
2 nein
3 Auszüge

r28 Urteilsbegründung
1 abgekürzt
2 Volle Begründung

r29 Anzahl der Seiten der Urteilsbegründung: ....

r30 Davon Seiten Beweiswürdigung: ....

r31 Wird in der Beweiswürdigung die Auskunftserteilung aufgegriffen?
1 ja
2 nein

r32 Mit welcher Beweisrichtung wird die Auskunftserteilung aufgegriffen?
1 Belastend (*voller Nachweis der Täterschaft*)
2 Belastend im Zusammenhang mit anderen Beweismitteln
3 Entlastend
4 Ohne Beweiskraft
0 Sonstiges: ....

r33 Stellenwert der Auskunftserteilung (*Einschätzung*): ....
....

Verfahrensauslösung

v001 Fall_Nr.*(Bearbeiternr.2stellig; Anzahl bearbeiteter Akten 3stellig: z.B.05025)*: ....

va1 Ermittlungsdelikt: ....

b01 Beschuldigten_Nr: ....

va2 Art der Kenntnisnahme/Entstehung des Tatverdachts
1 Anzeige-Opfer
2 Anzeige-Dritte
3 Hinweis-Dritte
4 Anzeige/Hinweis Behörden (*außerhalb Strafverfolgung*)
5 VP
6 Verdeckter Ermittler
7 Hinweise aus Auskunftserteilung
8 Hinweise aus TÜ
9 Hinweise aus Observation
10 Hinweise aus Lauschangriff
11 Hinweise aus Geständnis (*andere Beschuldigte*)
12 Anonymer Hinweis
13 Erkenntnisse aus anderen Verfahren
14 Zufallsfund: Hinweis aus TK-Daten ohne weitere TK-Daten-Anordnung
0 Sonstiges: ....

Erfolge

v001 Fall_Nr.:*(Bearbeiternr.2stellig; Anzahl bearbeiteter Akten 3stellig; z.B. 05025)*: ....

s01 Beschluss_Nr.: ....

e01 Wird die Auskunftserteilung in der Akte als erfolgreich eingestuft?
1 ja, wird ausdrücklich als erfolgreich eingestuft
2 ja, wird als bedingt erfolgreich eingestuft
3 Nein, ausdrücklich als nicht erfolgreich eingestuft

e02 Formulierung des Erfolges:
....

e03 Eigene Einschätzung des Erfolges
1 Auskunftserteilung war erfolgreich
2 Auskunftserteilung war bedingt erfolgreich
3 Auskunftserteilung war nicht erfolgreich

e04 Formulierung des Erfolges:
....

e05 Art des Erfolges
1 Identifizierung des Beschuldigten
2 Feststellung von (weiteren) Anschlüssen des Beschuldigten
3 Bestimmung des Standorts des Beschuldigten zur Tatzeit
4 Ermittlung des aktuellen Aufenthaltsortes des Beschuldigten
5 Bestimmung der Tatzeit
6 Bewegungsbild
7 Entlastung des Beschuldigten
8 Erweiterung des Tatvorwurfes
9 Weiterer Ermittlungsansatz wegen Katalogstraftat oder Straftat v. erh. Bedeutung
10 Weiterer Ermittlungsansatz wegen mittels Endeinrichtung begangener Straftat
11 Weiterer Ermittlungsansatz wegen sonstiger Straftat
12 Feststellung weiterer Tatbeteiligter bzw. ihrer Anschlüsse
13 Hinweise auf bislang unbekannte Straftaten anderer
14 Feststellung von Kommunikationspartnern des Beschuldigten
15 Feststellung Rufnummer/IP-Adresse für Folge-Auskunftserteilung
16 Feststellung, ob eine andere Ermittlungsmaßnahme in Betracht kommt
17 Sicherung von Beweisen (TK-Daten sind belastend)
18 TK-Daten sind belastend im Zusammenhang mit anderen Beweisen
0 Sonstige: ....

b01 Beschuldigten_Nr.: ....

e06 Details zur Identifizierung des Aufenthaltsorts
1 ja, endgültige Lokalisierung/Festnahme
2 Lokalisierung ja, aber kein erfolgreicher Zugriff

e07 wenn Hinweise auf neue Straftaten, welche? *(§§ angeben)* ....
....

e08 Verhältnis Dritter (Tatbeteiligter) zum Beschuldigten
1 Familie
2 Verwandtschaft
3 Freunde/Bekannte
4 Beruf-Arbeitgeber
5 Beruf-Arbeitskollegen
6 Szenebekanntschaft (Drogen)
7 Milieubekanntschaft
8 Ethnische Beziehungen (*gleiche Ethnie*)
9 Keine Beziehung

e09 Führen (auch) die (TK-Daten-)Erkenntnisse zu neuen Ermittlungsverfahren (gegen Besch./ Dritte) ? *(AZ;Verfahrensausgang)*: ....
....

e10 Führen (auch) die TK-Daten zu weiteren Ermittlungsansätzen bzw. -erkenntnissen?
1 ja
2 nein

e11 Wenn ja, zu welchen? ....
....

e12 Führen (mittelbare) Ermittlungsansätze/-erkenntnisse zu anderen Ermittlungsmaßnahmen?
1 Weitere Auskunftserteilung
2 TÜ
3 Durchsuchung
4 Beobachtung
5 Verdeckter Ermittler
6 V-Person
7 Beschlagnahme
8 Wohnraumüberwachung
9 Technische Mittel
10 Zeugenvernehmung
11 Fahndung
12 Rasterfahndung
0 Sonstiges

e13 Führt der mittelbar weiterführende Ermittlungsansatz zu Ermittlungserfolgen?
1 ja
2 nein
3 Ermittlungsansatz nicht weiterverfolgt/durchgeführt/vollzogen
0 Sonstiges:..

e14 Wenn ja, Erfolgsformulierung (*Stichworte; z.B. Auffinden von Beweismitteln*): ....
....

Maßnahmen

v001 Fall_Nr.(*Bearbeiternr.2stellig; Anzahl bearbeiteter Akten 3stellig; z.B.05025)*: ....

m01 Art der Maßnahme
1 TÜ
2 Durchsuchung
3 Beobachtung
4 Einsatz verdeckter Ermittler
5 V-Person
6 Beschlagnahme
7 Wohnraumüberwachung
8 Einsatz technischer Mittel
9 Zeugenvernehmung
10 Fahndung
11 Rasterfahndung
0 Sonstiges: ....

m02 bzgl. welcher Beschuldigten (Beschuldigten_Nr.): ....

m03 Wenn Zeugenvernehmung, Anzahl der Zeugen:..

m04 Datum des Beschlusses: ....

m05 Beginn der Maßnahme *(Datum)*: ....

m06 Ende der Maßnahme *(Datum)*: ....

m07 Ziel der Maßnahme: ....

m08 Erkenntnisse zur verfolgten Tat
1 ja
2 nein

m09 Art der Erkenntnisse zur verfolgten Tat
1 direkter Tatnachweis
2 direkte Tatdokumentation
3 Identifizierung des Beschuldigten
4 Feststellung von (weiteren) Anschlüssen des Beschuldigten
5 Bestimmung des Standorts des Beschuldigten zur Tatzeit
6 Ermittlung des aktuellen Aufenthaltsortes des Beschuldigten
7 Bestimmung der Tatzeit
8 Bewegungsbild
9 Entlastung des Beschuldigten
10 Erweiterung des Tatvorwurfes
11 Weiterer (mittelbarer) Ermittlungsansatz wegen Straftat von erheblicher Bedeutung
12 Weiterer (mittelbarer) Ermittlungsansatz wegen sonstiger Straftat
13 Feststellung weiterer Tatbeteiligter bzw. ihrer Anschlüsse
14 Hinweise auf bislang unbekannte Straftaten anderer
15 Feststellung von Kommunikationspartnern des Beschuldigten
16 Feststellung Rufnummer/IP-Adresse für Folge-Auskunftserteilung
17 Feststellung, ob eine andere Ermittlungsmaßnahme in Betracht kommt
18 Sicherung von Beweisen (TK-Daten sind belastend)
19 TK-Daten sind belastend im Zusammenhang mit anderen Beweisen
0 Sonstige: ....

m10 Einschätzung der Ergebnisse (Vergleich TK-Daten und andere Ermittlungsmaßnahmen):
....

m11 Erging in <u>einem</u> Beschluss eine Anordnung nach §§ 100g, 100h StPO und eine TKÜ? (AZ)

B. Fragebogen für die schriftliche Befragung

I. Berufliche Tätigkeit

I.1. Geschlecht	☐ männlich ☐ weiblich
I.2. Wie alt sind Sie?	_________ (*Jahre*)
I.3. Wie lange sind Sie schon bei der Staatsanwaltschaft tätig?	_________ (*Jahre*)
I.4. In welchem Dezernat sind Sie überwiegend tätig?	☐ Organisierte Kriminalität ☐ BtM ☐ Wirtschaftskriminalität ☐ Allgemeines Dezernat ☐ Sonstiges Dezernat: ....
I.5. Wie lange sind Sie schon in diesem Dezernat tätig?	_________ (*Jahre*)
I.6. Wie groß ist das Dezernat?	_________ *(Kollegen)*
I.7. In welchem Bundesland arbeiten Sie?	....
I.8. In welchem Landgerichtsbezirk sind Sie tätig?	....
I.9. Wie viele Verfahren mit Anordnungen nach §§ 100g, h StPO hatten Sie persönlich im Jahr 2005?	_________ *(Verfahren)*

II. Delikte und Verdachtsgrad

Die nachfolgenden Fragestellungen beziehen sich auf die Straftatbestände, die *Ihren Anträgen* nach §§ 100g, 100h StPO zugrunde liegen sowie den für die Anordnung erforderlichen Verdachtsgrad.

II.1. Bitte schätzen Sie, ob und in welchem Umfang Ihren Anträgen im Jahr 2005 folgende Straftatbestände zugrunde lagen:	Fallzahl	Ist nach Ihrer Einschätzung die Tendenz zum Vorjahr steigend	gleich bleibend	fallend ?
a) Straftaten von erheblicher Bedeutung				
○ Politische Delikte (Friedensverrat, usw.) →	________	☐	☐	☐
○ Vereinigungsdelikte (z.B. § 129 StGB) →	________	☐	☐	☐
○ Fälschungsdelikte →	________	☐	☐	☐
○ Sexueller Missbrauch von Kindern →	________	☐	☐	☐
○ Verbreitung pornografischer Schriften →	________	☐	☐	☐
○ Tötungsdelikte →	________	☐	☐	☐
○ Straftaten gegen die persönliche Freiheit (Menschenhandel, Geiselnahme, usw.) →	________	☐	☐	☐
○ Diebstahl (§§ 242,243,244,244 a StGB) →	________	☐	☐	☐
○ Raub, räuberische Erpressung →	________	☐	☐	☐
○ Erpressung →	________	☐	☐	☐
○ Hehlerei →	________	☐	☐	☐

		Fallzahl	steigend	gleich bleibend	fallend ?
○	Geldwäsche →	________	☐	☐	☐
○	Gemeingefährliche Straftaten →	________	☐	☐	☐
		Fallzahl	steigend	gleich bleibend	fallend ?
○	Verstöße gegen das Waffengesetz →	________	☐	☐	☐
○	Verstöße gegen das AußenwirtschaftsG →	________	☐	☐	☐
○	Betäubungsmitteldelikte →	________	☐	☐	☐
○	Verstöße gegen das Ausländerrecht →	________	☐	☐	☐
○	Betrug →	________	☐	☐	☐
○	Sexueller Missbrauch, sexuelle Nötigung, Vergewaltigung →	________	☐	☐	☐
○	Androhung von Straftaten, § 126 StGB →	________	☐	☐	☐
○	Körperverletzung →	________	☐	☐	☐
○	Nötigung →	________	☐	☐	☐
○	Entziehung Minderjähriger →	________	☐	☐	☐
○	Sonstige Straftaten von erheblicher Bedeutung: .... →	________	☐	☐	☐
	.... →	________	☐	☐	☐
b) Mittels einer Endeinrichtung begangene Straftaten			Tendenz zum Vorjahr		
		Fallzahl	steigend	gleich bleibend	fallend ?
○	Beleidigung mittels Telefon, Fax, E-Mail, SMS →	________	☐	☐	☐
○	Bedrohung mittels Telefon, usw. →	________	☐	☐	☐
○	Telefonterror, Versendung von E-Mails in Massen →	________	☐	☐	☐
○	Sexuell belästigende Anrufe, E-Mails oder SMS →	________	☐	☐	☐
○	Verbreitung pornografischer oder rechtsradikaler Bilder, Schriften etc. →	________	☐	☐	☐
○	Computerbetrug →	________	☐	☐	☐
○	Datenveränderung, Computersabotage →	________	☐	☐	☐
○	Datenfälschung →	________	☐	☐	☐
○	Ausspähen von Daten (§ 202a StGB) →	________	☐	☐	☐
○	Missbrauch von Notrufen →	________	☐	☐	☐
○	Warenbestellbetrug →	________	☐	☐	☐
○	Urheberrechtsverletzungen (z.B. Softwarepiraterie) →	________	☐	☐	☐
○	Sonstige mittels Endeinrichtung begangene				

<table>
<tr><td>Straftaten: .... →
.... →</td><td>________ ☐ ☐ ☐
________ ☐ ☐ ☐</td></tr>
<tr><td colspan="2">Die derzeitige Regelung des § 100g Abs. 1 Satz 1 StPO sieht vor, dass bestimmte Tatsachen den Verdacht einer Straftat von erheblicher Bedeutung oder einer mittels Endeinrichtung begangenen Straftat begründen müssen.</td></tr>
<tr><td>II.2. Halten Sie den gesetzlich festgelegten Verdachtsgrad für angemessen?</td><td>☐ Ja, weil ....
....
....
☐ Nein, weil ....
....
....</td></tr>
<tr><td colspan="2">Gemäß § 100g Abs. 1 Satz 1 StPO wird für die Anordnung einer Auskunftserteilung die Begehung einer Straftat von erheblicher Bedeutung, insbesondere einer der in § 100a Satz 1 StPO genannten Straftaten, vorausgesetzt.</td></tr>
<tr><td>II.3. Halten Sie Änderungen diesbezüglich für angezeigt?</td><td>☐ Ja ☐ Nein
Wenn ja, welche Änderungen würden Sie befürworten:
☐ Der Gesetzeswortlaut sollte sich auf Katalogstraftaten i.S.v. § 100a Satz 1 StPO beschränken und der Begriff „Straftat von erheblicher Bedeutung“ sollte gestrichen werden.
☐ Es sollte nur die allg. Formulierung „Straftat von erheblicher Bedeutung“ gewählt werden.
☐ Sonstige Änderungen: ....
....
....</td></tr>
<tr><td colspan="2">Im Schrifttum ist umstritten, ob es sich bei einer Straftatbegehung mittels Endeinrichtung auch um eine erhebliche Straftat handeln muss, damit eine Auskunftsanordnung ergehen kann.</td></tr>
<tr><td>II.4. Wie verstehen Sie den § 100g Abs. 1 Satz 1 StPO in Bezug auf diesen Aspekt?</td><td>☐ Ja, es muss eine erhebliche Straftat vorliegen, weil ....
....
....
☐ Nein, es muss sich um keine erhebliche Straftat handeln, weil ....
....
....</td></tr>
</table>

Anmerkungen:

III. Verhältnis zu anderen Ermittlungsmaßnahmen

In den nächsten Fragen bitten wir Sie um Ihre *allgemeine Einschätzung* zum Verhältnis von Maßnahmen nach §§ 100g, 100h StPO zu anderen Ermittlungsmaßnahmen. *(Verhältnis speziell zur TKÜ siehe Abschnitt IV.)*

III.1. Wie häufig wurden Ihrer Einschätzung nach Auskunftsersuchen nach §§ 100g, 100h StPO im Jahr 2005 im selben Verfahren mit anderen Ermittlungsmaßnahmen kombiniert?

	immer	häufig	gelegentlich	selten	nie
Beschlagnahme →	☐	☐	☐	☐	☐
Postbeschlagnahme →	☐	☐	☐	☐	☐
(Raster-)Fahndung →	☐	☐	☐	☐	☐
Wohnraumüberwachung →	☐	☐	☐	☐	☐
Einsatz technischer Mittel →	☐	☐	☐	☐	☐
Durchsuchung →	☐	☐	☐	☐	☐
Einsatz verdeckter Ermittler →	☐	☐	☐	☐	☐
Observation →	☐	☐	☐	☐	☐
Sonstige, nämlich .... →	☐	☐	☐	☐	☐
.... →	☐	☐	☐	☐	☐

III.2. In welchem zeitlichen Zusammenhang standen dabei die Auskunftsersuchen i.d.R. mit solchen anderen Ermittlungsmaßnahmen?

- ☐ Auskunftsersuchen erfolgte früher
- ☐ Maßnahmen ergingen zeitgleich
- ☐ Auskunftsersuchen erfolgte später

III.3. Welche typischen Fallkonstellationen gibt es bei der kombinierten Anwendung der Auskunftserteilung mit anderen Ermittlungsmaßnahmen?

	immer	häufig	gelegentlich	selten	nie
Beschlagnahme von Verbindungsdaten	☐	☐	☐	☐	☐
Durchsuchung, um Verbindungsdaten zu finden	☐	☐	☐	☐	☐
Sonstige, nämlich	☐	☐	☐	☐	☐
....	☐	☐	☐	☐	☐
....	☐	☐	☐	☐	☐
....	☐	☐	☐	☐	☐

Anmerkungen:

IV. Verhältnis speziell zur TKÜ

IV.1. Wie häufig wurden Auskunftsersuchen nach §§ 100g, 100h StPO im Jahr 2005 mit TKÜ-Maßnahmen kombiniert?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie
IV.2. In welchem zeitlichen Zusammenhang standen dabei die Auskunftsersuchen i.d.R. mit den TKÜ-Maßnahmen?	☐ Auskunftsersuchen erfolgte früher ☐ Maßnahmen ergingen zeitgleich ☐ Auskunftsersuchen erfolgte später
IV.3. Wie beurteilen Sie die Erfolgsaussichten der kombinierten Anwendung von Auskunftserteilung und TKÜ?	☐ sehr hoch ☐ hoch ☐ mittelmäßig ☐ niedrig ☐ sehr niedrig
IV.4. In welchem ermittlungspraktischen Verhältnis stehen die Maßnahmen Ihrer Erfahrung nach zueinander? *(Zutreffendes bitte ankreuzen; Mehrfachantworten möglich)*	☐ Auskunftserteilung ist kostengünstiger ☐ Auskunftserteilung ist erfolgversprechender ☐ Auskunftserteilung ist schneller ☐ Auskunftserteilung ist einfacher auszuwerten ☐ Auskunftserteilung führt zu stichhaltigeren Beweisen ☐ Auskunftserteilung wird öfter vom Richter bewilligt als die TKÜ ☐ Auskunftserteilung ist in bestimmten Fallkonstellationen sinnvoller als die TKÜ:...... .... ☐ Auskunftserteilung ist bei bestimmten Delikten sinnvoller als die TKÜ: .... ☐ TKÜ erfordert mehr Arbeitsaufwand ☐ TKÜ ist eingriffsintensiver ☐ TKÜ führt zu stichhaltigeren Beweisen

	☐ TKÜ betrifft weniger Personen ☐ TKÜ ist erfolgversprechender ☐ TKÜ ist in bestimmten Fallkonstellationen sinnvoller als die Auskunftserteilung:......... .... ☐ TKÜ ist bei bestimmten Delikten sinnvoller als die Auskunftserteilung:........................... .... ☐ Sonstiges: ....
IV.5. Gibt es Ihrer Ansicht nach rechtliche oder praktische Verbesserungsmöglichkeiten bei der kombinierten Anwendung einer Maßnahme nach §§ 100g, 100h StPO und einer TKÜ?	☐ Ja ☐ Nein Wenn ja, welche: ....
Anmerkungen:	

V. Antragstellung

Die folgenden Fragestellungen betreffen die Beantragung der Auskunftserteilung nach §§ 100g, 100h StPO.	
V.1. Vom wem geht Ihrer Erfahrung nach in welchem Umfang die Initiative zur Antragstellung aus?	☐ Polizei zu .... % ☐ Staatsanwaltschaft zu .... % = 100%

V.2. In welchen staatsanwaltschaftlichen Abteilungen werden die Maßnahmen nach Ihren Erfahrungen beantragt bzw. angeordnet?	immer	häufig	gelegentlich	selten	nie
Organisierte Kriminalität	☐	☐	☐	☐	☐
Betäubungsmitteldelikte	☐	☐	☐	☐	☐
Wirtschaftsdelikte	☐	☐	☐	☐	☐
Andere, nämlich:	☐	☐	☐	☐	☐
....	☐	☐	☐	☐	☐
V.3. Wie häufig spielen folgende kriminalistische Ziele eine Rolle für die Antragstellung:	immer	häufig	gelegentlich	selten	nie
Identifizierung des Beschuldigten	☐	☐	☐	☐	☐
Feststellung von (weiteren) Anschlüssen des Beschuldigten	☐	☐	☐	☐	☐
Bestimmung des Standorts des Beschuldigten zur Tatzeit	☐	☐	☐	☐	☐
Ermittlung des aktuellen Standorts des Beschuldigten	☐	☐	☐	☐	☐
Bestimmung der Tatzeit	☐	☐	☐	☐	☐
Feststellung von Kommunikationspartnern des Beschuldigten	☐	☐	☐	☐	☐
Feststellung weiterer Tatbeteiligter	☐	☐	☐	☐	☐
Erlangung von Beweismitteln für tatbestandsmäßiges Verhalten	☐	☐	☐	☐	☐
Feststellung, ob eine TKÜ erfolgversprechend sein könnte	☐	☐	☐	☐	☐
Feststellung, ob eine andere Ermittlungsmaßnahme als eine TKÜ in Betracht kommt	☐	☐	☐	☐	☐
Bekämpfung der Datennetzkriminalität	☐	☐	☐	☐	☐
Andere, nämlich:	☐	☐	☐	☐	☐
Anmerkungen:					

VI. Anordnungen

Im Folgenden möchten wir Ihre *allgemeine Einschätzung* zu der Zahl der Anordnungen nach §§ 100g, 100h StPO im Jahr 2005 sowie Ihre Meinung zum Richtervorbehalt in Erfahrung bringen.			
VI.1. Wie hoch war Ihrer Einschätzung nach im Jahr 2005 der Anteil der richterlichen bzw. staatsanwaltschaftlichen Anordnungen?	Eigenerfahrung	Schätzung für die Abteilung	Schätzung für die Behörde insg.
Anordnungen durch den Richter	.... %	.... %	.... %
Eilanordnungen durch die Staatsanwaltschaft	.... %	.... %	.... %
	= 100 %	= 100 %	= 100 %
VI.2. Wie schätzen Sie dabei den Anteil der staatsanwaltschaftlichen Anordnungen im Vergleich zum Vorjahr ein?	Tendenz steigend ☐	gleich bleibend ☐	fallend ☐
VI.3. Wann erfolgt nach einer Eilanordnung in der Regel die richterliche Bestätigung?	☐ am Tag der Eilanordnung ☐ am nächsten Tag ☐ am übernächsten Tag ☐ am dritten Tag nach der Eilanordnung		
VI.4. Wie beurteilen Sie den Richtervorbehalt im Hinblick auf die Ermittlungstätigkeit der Ermittlungsbehörden?	☐ sinnvoll ☐ eher sinnvoll ☐ eher nicht sinnvoll ☐ nicht sinnvoll		
VI.5. Sollte der Richtervorbehalt in Zukunft ... ?	☐ erweitert werden ☐ unverändert beibehalten werden ☐ eingeschränkt werden		
Anmerkungen:			

VII. Ablehnung von Anträgen und Eilanordnungen

In diesem Abschnitt möchten wir Sie bitten, *allgemein einzuschätzen*, in welchem Maße eine Ablehnung von Anträgen und Eilanordnungen der Staatsanwaltschaft durch den Richter erfolgt.

VII.1. In welchem Umfang werden Anträge auf Auskunftserteilung abgelehnt?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie

VII.2. Mit welcher Begründung werden die Anträge abgelehnt?	immer	häufig	gelegentlich	selten	nie
Kein ausreichender Tatverdacht	☐	☐	☐	☐	☐
Keine Straftat von *erheblicher* Bedeutung	☐	☐	☐	☐	☐
Milderes Mittel anwendbar	☐	☐	☐	☐	☐
Maßnahme verspricht keinen Erfolg	☐	☐	☐	☐	☐
Sonstiges:	☐	☐	☐	☐	☐
....	☐	☐	☐	☐	☐

VII.3. In welchem Umfang werden nach Ihrer Einschätzung staatsanwaltschaftliche Eilanordnungen vom Richter bestätigt?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie
VII.4. In welchem Umfang werden Maßnahmen gemäß §§ 100g, 100h StPO nach Ihrer Erfahrung, bevor der Antrag auf Auskunftserteilung überhaupt gestellt wurde, im Rahmen einer informellen Besprechung mit dem Richter abgelehnt?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie
Anmerkungen:	

VIII. Dauer der Maßnahmen

Bei den folgenden Fragen bitten wir Sie, *Schätzungen* bzgl. der Dauer der Ermittlungsmaßnahme sowie der dabei auftretenden Unterschiede zwischen Antrag, Anordnung und tatsächlicher Durchführung abzugeben.

VIII.1. Welche Dauer beantragen Sie durchschnittlich für die Durchführung der Maßnahmen, wenn sich die Auskunftserteilung	1 Monat	2 Monate	3 Monate	bis 6 Monate	länger
a) auf *vorhandene* TK-Verbindungsdaten (§ 100g Abs. 1 Satz 1, Abs. 3 StPO) richtet?	☐	☐	☐	☐	☐
b) auf *zukünftige* TK-Verbindungsdaten (§ 100g Abs. 1 Satz 3, Abs. 3 StPO) richtet?	☐	☐	☐	☐	☐
c) auf eine *Zielwahlsuche* (§ 100g Abs. 2 StPO) richtet?	☐	☐	☐	☐	☐

VIII.2. Wie stellt sich die tatsächlich *angeordnete* Dauer im Vergleich zu der von Ihnen *beantragten* Dauer dar?	immer	häufig	gelegentlich	selten	nie
kürzer	☐	☐	☐	☐	☐
so wie beantragt	☐	☐	☐	☐	☐
länger	☐	☐	☐	☐	☐

VIII.3. Wie oft entspricht die *angeordnete* der *tatsächlichen* Dauer der Maßnahme?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie
VIII.4. In welchem Umfang haben Sie im Jahr 2005 Verlängerungen beantragt?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie
VIII.5. Wie oft werden Verlängerungen vom Richter abgelehnt?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie
Anmerkungen:	

IX. Durchführung der Maßnahmen

In diesem Teil des Fragebogens möchten wir die von Ihnen festgestellten Schwierigkeiten bei der Durchführung der Auskunftserteilung in Erfahrung bringen.					
IX.1. Ist es im Jahr 2005 zu folgenden Schwierigkeiten bei der Inanspruchnahme der TK-Anbieter gekommen, die den Erfolg des Auskunftsverlangens beeinträchtigt haben?	immer	häufig	gelegentlich	selten	nie
Verzögerungen	☐	☐	☐	☐	☐
Nichtakzeptierung von Anordnungen	☐	☐	☐	☐	☐
Daten wurden von vornherein nicht gespeichert, d.h. sofort gelöscht	☐	☐	☐	☐	☐
Daten wurden nur teilanonymisiert gespeichert	☐	☐	☐	☐	☐
Daten wurden nicht lange genug gespeichert, d.h. zu früh gelöscht	☐	☐	☐	☐	☐
Sonstiges, nämlich	☐	☐	☐	☐	☐
....	☐	☐	☐	☐	☐
IX.2. Auf welche Gründe führen Sie diese Schwierigkeiten zurück?	....				
IX.3. Welche Folgen sind daraus entstanden?	immer	häufig	gelegentlich	selten	nie
Beschuldigter konnte nicht identifiziert werden	☐	☐	☐	☐	☐
Anschluss des Beschuldigten konnte ihm nicht (mehr) zugeordnet werden	☐	☐	☐	☐	☐
Beteiligte konnten nicht identifiziert werden	☐	☐	☐	☐	☐
Maßnahme konnte nicht durchgeführt werden	☐	☐	☐	☐	☐
Auskunftsersuchen blieb erfolglos	☐	☐	☐	☐	☐
Verfahrensverzögerungen	☐	☐	☐	☐	☐
Sonstiges, nämlich	☐	☐	☐	☐	☐
....	☐	☐	☐	☐	☐
IX.4. In welchem Umfang wurde die Durch- führung von Auskunftsverlangen im Jahr 2005 durch die Verwendung von Verschlüsselungs-techniken (Anonymisierungsdienste, Kryptographie) beeinflusst?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie				

IX.5. Welche Folgen hatte dies für den Erfolg des Auskunftsverlangens?	immer	häufig	gelegentlich	selten	nie
Beschuldigter konnte nicht identifiziert werden	☐	☐	☐	☐	☐
Anschluss des Beschuldigten konnte ihm nicht (mehr) zugeordnet werden	☐	☐	☐	☐	☐
Beteiligte konnten nicht identifiziert werden	☐	☐	☐	☐	☐
Maßnahme konnte nicht durchgeführt werden	☐	☐	☐	☐	☐
Auskunftsersuchen blieb erfolglos	☐	☐	☐	☐	☐
Verfahrensverzögerungen	☐	☐	☐	☐	☐
Sonstiges, nämlich	☐	☐	☐	☐	☐
....	☐	☐	☐	☐	☐

IX.6. Wie beurteilen Sie die Zusammenarbeit bei der Durchführung der Maßnahmen?	sehr gut	gut	mittel-mäßig	schlecht	sehr schlecht
zwischen StA und Polizei	☐	☐	☐	☐	☐
zwischen StA und Richter	☐	☐	☐	☐	☐
zwischen StA und TK-Anbieter	☐	☐	☐	☐	☐

Auf EU-Ebene hat das Europäische Parlament Ende 2005 beschlossen, dass sämtliche Verbindungsdaten der Telekommunikationsnutzer für eine Dauer von 6 Monaten bis zu 2 Jahren gespeichert werden sollen.

IX.7. Für welchen Zeitraum halten Sie die Speicherung von Verbindungsdaten für sinnvoll?	☐ keine Datenspeicherung ☐ Speicherung für 1 bis 6 Monate ☐ Speicherung für 6 bis 12 Monate ☐ Speicherung bis zu 2 Jahren ☐ unbefristete Speicherung aller Daten
IX.8. Gibt es Fälle, in denen eine Maßnahme nach §§ 100g, 100h StPO angeordnet wird, obwohl eine andere mildere Maßnahme ebenso erfolgversprechend gewesen wäre?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie Bitte begründen Sie Ihre Antwort: ....

Anmerkungen:

X. Benachrichtigung der Betroffenen

Gemäß § 101 Abs. 1 StPO sind die Beteiligten von den getroffenen Maßnahmen zu benachrichtigen, sobald dies ohne Gefährdung u.a. des Untersuchungszwecks und der öffentlichen Sicherheit geschehen kann.	
X.1. Wie hoch ist Ihrer Erfahrung nach die durchschnittliche Anzahl der grundsätzlich zu benachrichtigenden Betroffenen je Anordnung?	☐ 1 Person ☐ 2 Personen ☐ 3 bis 5 Personen ☐ 6 bis 10 Personen ☐ mehr als 10 Personen
X.2. Wie hoch ist nach Ihrer Einschätzung der Anteil nicht benachrichtigter Betroffener? (100 % ist die Anzahl der Betroffenen insgesamt)	.... %
X.3. Wie hoch ist der Anteil der Zurückstellung der Benachrichtigung nach § 101 Abs. 1 StPO? (100 % ist die Anzahl der Betroffenen insgesamt)	.... %
X.4. Was sind Ihrer Meinung nach die Gründe für die Nichtbenachrichtigung oder die Zurückstellung der Benachrichtigung?	....
X.5. Sollte Ihrer Meinung nach die Benachrichtigungspflicht ... ?	☐ erweitert werden ☐ beibehalten werden ☐ eingeschränkt werden ☐ abgeschafft werden

XI. Zeugnisverweigerungsrechte

Ein Auskunftsverlangen ist gemäß § 100h Abs. 2 Satz 1 StPO unzulässig, wenn ein Betroffener ein Zeugnisver-weigerungsrecht gemäß § 53 Abs. 1 Satz 1 Nr. 1, 2 und 4 StPO hat. Die Unzulässigkeit der Maßnahme ergibt sich demnach nur bei Geistlichen, Verteidigern sowie Mitgliedern gesetzgebender Körperschaften. Andere nach §§ 52, 53, 53a StPO zeugnisverweigerungsberechtigte Personen sind nicht von § 100h Abs. 2 StPO erfasst.

XI.1. Wie oft sind Ihrer *allgemeinen Einschätzung* nach folgende zeugnisverweigerungsberechtigte Personen i. S. v. §§ 52, 53, 53a StPO von den Maßnahmen betroffen:	immer	häufig	gelegentlich	selten	nie
Angehörige i.S.v. § 52 StPO	☐	☐	☐	☐	☐
Geistliche	☐	☐	☐	☐	☐
Verteidiger des Beschuldigten	☐	☐	☐	☐	☐
Rechtsanwälte, Patentanwälte, Notare	☐	☐	☐	☐	☐
Wirtschaftsprüfer, Steuerberater	☐	☐	☐	☐	☐
Ärzte	☐	☐	☐	☐	☐
Psychotherapeuten	☐	☐	☐	☐	☐
Apotheker, Hebammen	☐	☐	☐	☐	☐
Berater für Betäubungsmittelabhängigkeit	☐	☐	☐	☐	☐
Mitglieder des Bundestages oder eines Landtages	☐	☐	☐	☐	☐
Journalisten	☐	☐	☐	☐	☐
Berufshelfer i.S.v. § 53a StPO	☐	☐	☐	☐	☐

Es ist eine Vereinheitlichung der Vorschriften über verdeckte Ermittlungsmaßnahmen in Bezug auf Zeugnisverweigerungsrechte geplant.

XI.2. Sollten Ihrer Meinung nach alle Zeugnisverweigerungsberechtigten i.S.v. §§ 52, 53, 53a StPO in den einschlägigen Normen einheitlich berücksichtigt werden?	☐ Ja, weil .... ☐ Nein, weil ....

Anmerkungen:

XII. Kosten und technische Umsetzung

In den nachfolgenden Fragen interessieren wir uns für die technische Umsetzung der Maßnahmen nach §§ 100g, 100h StPO sowie die dadurch entstehenden Kosten.

XII.1. Wie hoch schätzen Sie die tatsächlichen Kosten für die Durchführung der Maßnahmen, die den Netzbetreibern entstehen, ein? Bitte versuchen Sie einen konkreten Betrag anzugeben: .... EUR	☐ sehr hoch ☐ hoch ☐ eher hoch ☐ eher niedrig ☐ niedrig ☐ sehr niedrig
XII.2. Spielt der Kostenaspekt für Sie eine Rolle bei der Beantragung der Auskunftserteilung?	☐ Ja, weil .... ☐ Nein, weil ....
XII.3. Wurde die Durchführung von Auskunftsverlangen im Jahr 2005 durch technische Probleme beeinträchtigt?	☐ immer ☐ häufig ☐ gelegentlich ☐ selten ☐ nie
XII.4. Um welche technischen Probleme handelte es sich dabei?	....

XII.5. In welchem Maße wurde dadurch der Erfolg der Maßnahme beeinflusst?	immer	häufig	gelegentlich	selten	nie
Beschuldigter konnte nicht identifiziert werden	☐	☐	☐	☐	☐
Anschluss des Beschuldigten konnte ihm nicht (mehr) zugeordnet werden	☐	☐	☐	☐	☐
Beteiligte konnten nicht identifiziert werden	☐	☐	☐	☐	☐
Maßnahme konnte nicht durchgeführt werden	☐	☐	☐	☐	☐
Auskunftsersuchen blieb erfolglos	☐	☐	☐	☐	☐
Verfahrensverzögerungen	☐	☐	☐	☐	☐
Sonstiges, nämlich	☐	☐	☐	☐	☐

Anmerkungen:

XIII. Normanwendungsprobleme

Im Folgenden geht es um spezielle Schwierigkeiten, die im Rahmen Ihrer Tätigkeit bei der Anwendung der §§

<table>
<tr><td colspan="2">100g, 100h StPO aufgetreten sein könnten.</td></tr>
<tr><td>XIII.1. Falls Sie Auskünfte über Personendaten zu dynamischen IP-Adressen eingeholt haben: Aufgrund welcher Rechtsgrundlage taten Sie dies?</td><td>..
....
....</td></tr>
<tr><td>XIII.2. Hat es dabei Schwierigkeiten gegeben?</td><td>☐ Ja, es sind folgende Schwierigkeiten aufgetreten: ....
....
....
....
....
☐ Nein</td></tr>
<tr><td colspan="2">Die Vorschrift des § 100h Abs. 1 Satz 1 StPO sieht vor, dass bei der Anordnung der Maßnahme Name und Anschrift des Betroffenen sowie die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses anzugeben sind. Nur im Falle einer Straftat von erheblicher Bedeutung genügt gemäß § 100h Abs. 1 Satz 2 StPO eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn andernfalls die Erforschung des Sachverhalts aussichtslos oder wesentlich erschwert wäre.</td></tr>
<tr><td>XIII.3. Sollte Ihrer Meinung nach die Ausnahmeregelung des § 100h Abs. 1 Satz 2 StPO</td><td>☐ erweitert werden
☐ in ihrer jetzigen Fassung beibehalten werden
☐ eingeschränkt werden
Bitte begründen Sie Ihre Antwort:
....
....
....</td></tr>
<tr><td>XIII.4. Wie oft können Straftaten, die nicht von erheblicher Bedeutung sind, wegen dieser Regelung nicht aufgeklärt werden?</td><td>☐ immer
☐ häufig
☐ gelegentlich
☐ selten
☐ nie</td></tr>
<tr><td colspan="2">Anmerkungen:</td></tr>
</table>

XIV. Häufigkeit der Maßnahmen

<table>
<tr><td colspan="4">Bei den nachfolgenden Fragen bitten wir Sie, sofern es Ihnen möglich ist, eine ungefähre Schätzung der Häufigkeit der Maßnahmen in Ihrer Behörde abzugeben.</td></tr>
<tr><td>XIV.1. Wie viele Maßnahmen nach §§ 100g, 100h StPO wurden im Jahr 2005 beantragt? (Fallzahl)</td><td>Eigenerfahrung

..................</td><td>Schätzung für die Abteilung

..................</td><td>Schätzung für die Behörde insg.

..................</td></tr>
</table>

XIV.2. Konnten Sie dabei im Rahmen Ihrer Tätigkeit eine Veränderung zum Vorjahr feststellen?	Tendenz zum Vorjahr steigend ☐	 gleich bleibend ☐	 fallend ☐
XIV.3. Wie viele Anordnungen nach §§ 100g, 100h StPO wurden im Jahr 2005 *erlassen*? *(Fallzahl)*	Eigenerfahrung	Schätzung für die Abteilung	Schätzung für die Behörde insg. ....
XIV.4. Konnten Sie dabei im Rahmen Ihrer Tätigkeit eine Veränderung zum Vorjahr feststellen?	Tendenz zum Vorjahr steigend ☐	 gleich bleibend ☐	 fallend ☐
XIV.5. Wie verteilen sich die *Anträge* auf Auskunftserteilung nach Ihrer Einschätzung prozentual	Eigenerfahrung	Schätzung für die Abteilung	Schätzung für die Behörde insg.
a) auf *vorhandene* TK-Verbindungsdaten (§ 100g Abs. 1 Satz 1, Abs. 3 StPO)?	.....................(%)	....................(%)	.....................(%)
b) auf *zukünftige* TK-Verbindungsdaten (§ 100g Abs. 1 Satz 3, Abs. 3 StPO)?	.....................(%)	....................(%)	.....................(%)
c) auf die *Zielwahlsuche* (§ 100g Abs. 2 StPO)?	.....................(%)	....................(%)	.....................(%)
	= 100%	= 100%	= 100%
XIV.6. Wie verteilen sich die Auskunfts*anordnungen* nach Ihrer Einschätzung prozentual	Eigenerfahrung	Schätzung für die Abteilung	Schätzung für die Behörde insg.
a) auf *vorhandene* TK-Verbindungsdaten (§ 100g Abs. 1 Satz 1, Abs. 3 StPO)?	.....................(%)	....................(%)	.....................(%)
b) auf *zukünftige* TK-Verbindungsdaten (§ 100g Abs. 1 Satz 3, Abs. 3 StPO)?	.....................(%)	....................(%)	.....................(%)
c) auf die *Zielwahlsuche* (§ 100g Abs. 2 StPO)?	.....................(%)	....................(%)	.....................(%)
	= 100%	= 100%	= 100%
Die folgende Frage betrifft die möglichen Kombinationen der einzelnen Anwendungsfälle der Auskunftserteilung und die Häufigkeit einer gleichzeitigen Anwendung.			

XIV.7. Wie verteilen sich die Auskunfts*anordnungen* Ihrer Einschätzung nach prozentual	Eigenerfahrung	Schätzung für die Abteilung	Schätzung für die Behörde insg.
a) auf *vorhandene* in Kombination mit *zukünftigen* TK-Verbindungsdaten?	....................(%)	....................(%)	....................(%)
b) auf *vorhandene* TK-Verbindungsdaten in Kombination mit *Zielwahlsuche*?	....................(%)	....................(%)	....................(%)
c) auf *zukünftige* TK-Verbindungsdaten in Kombination mit *Zielwahlsuche*?	....................(%)	....................(%)	....................(%)
d) auf eine Kombination von *vorhandenen* und *zukünftigen* TK-Verbindungsdaten sowie der *Zielwahlsuche*?	....................(%)	....................(%)	....................(%)
	= 100%	= 100%	= 100%

XV. Erfolgsaussichten

XV.1. Wie schätzen Sie die *Erfolgsquote* der Maßnahmen im Hinblick auf die Bedeutung der Daten für den weiteren Verfahrensgang allgemein ein? Und zwar bei Auskunftserteilung	Die Erfolgsaussichten (Erfolg als jegliches Erlangen ermittlungsrelevanter Erkenntnisse) sind: hoch	eher hoch	eher niedrig	niedrig
a) bezogen auf *vorhandene* TK-Verbindungsdaten (§ 100g Abs. 1 Satz 1, Abs. 3 StPO)?	☐	☐	☐	☐
b) bezogen auf *zukünftige* TK-Verbindungsdaten (§ 100g Abs. 1 Satz 3, Abs. 3 StPO)?	☐	☐	☐	☐
c) bezogen auf die *Zielwahlsuche* (§ 100g Abs. 2 StPO)?	☐	☐	☐	☐
d) bezogen auf *vorhandene* in Kombination mit *zukünftigen* TK-Verbindungsdaten?	☐	☐	☐	☐
e) bezogen auf *vorhandene* TK-Verbindungsdaten in Kombination mit *Zielwahlsuche*?	☐	☐	☐	☐
f) bezogen auf *zukünftige* TK-Verbindungsdaten in Kombination mit *Zielwahlsuche*?	☐	☐	☐	☐
g) bezogen auf eine Kombination von *vorhandenen* und *zukünftigen* TK-Verbindungsdaten sowie der *Zielwahlsuche*?	☐	☐	☐	☐

XVI. Zusammenfassende Fragestellungen

Bis zum 31.12.2001 war die Auskunftserteilung über Telekommunikationsverbindungsdaten nicht in der StPO, sondern in § 12 FAG geregelt.	
XVI.1. Haben sich nach Ihrer Erfahrung durch die Neuregelungen in den §§ 100g, 100h StPO gegenüber der alten Rechtslage (§ 12 FAG) Änderungen für die Praxis ergeben?	☐ Ja ☐ Nein Wenn ja, welche: ☐ höhere Anzahl an Anordnungen ☐ geringere Anzahl an Anordnungen ☐ mehr Erfolge ☐ weniger Erfolge ☐ sonstiges, nämlich ....
XVI.2. Gibt es aus Ihrer Sicht Unklarheiten bzgl. des Regelungsgehalts der §§ 100g, 100h StPO? (z.B. welche Daten erhoben werden dürfen)	☐ Ja ☐ Nein Wenn ja, welche: ....
XVI.3. Wie schätzen Sie die praktische Bedeutung der Auskunftserteilung für Ihre Tätigkeit ein?	☐ hoch ☐ eher hoch ☐ eher gering ☐ gering
Die Geltungsdauer der derzeitigen Normen (§§ 100g, 100h StPO) ist zeitlich befristet bis zum 31.12.2007.	
XVI.4. Welche Auswirkungen hätte es Ihrer Ansicht nach, wenn die Regelungen der §§ 100g, 100h StPO Ende des Jahres 2007 nicht verlängert werden würden? *(Zutreffendes bitte ankreuzen; Mehrfachantworten möglich)*	☐ Das wäre kein Verlust. ☐ Die Auskunftserteilung kann durch häufigere Anwendung anderer Ermittlungsmaßnahmen, insb. der TKÜ, ersetzt werden. ☐ Die Auskunftserteilung ist nicht ersetzbar durch andere Ermittlungsmaßnahmen. ☐ Die Maßnahmen nach §§ 100g, 100h StPO sind unverzichtbar. ☐ Sonstiges:... ....
Schlussbemerkungen:	



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333